Using Modular Open Systems Approach (MOSA) to Address System Survivability in Army Weapon Systems

Terance F. Carlson
Fellow

Defense Acquisition University (DAU) – South Region
Senior Service College Fellowship 2018-2019
Huntsville, Alabama

6 May 2019

This research paper presented to the Defense Acquisition University for partial fulfillment of the academic requirements for the Army's Senior Service College Fellowship (SSCF) under the direction of SSCF Director, Mr. William A. Colson, and Research Advisor, Mr. Steve Mills.

Approval Page

Title: Using Modular Open Systems Approach (MOSA) to Address System Survivability in Army Weapon Systems
Author: Terance F. Carlson
Organization: DAU-South, Senior Service College Fellowship (SSCF)
Date of Paper: 6 May 2019

Research Advisor: Mr. Steve Mills — Approval Date: 10 Apr 2019
Research Lead: Ms. Dana Stewart — Approval Date: 19 April 2019
SSCF Director: Mr. Bill Colson — Approval Date: 6 May 2019
OPSEC Approval – 6 May 2019

Disclaimer

The views and opinions expressed or implied in this research paper are those of the author; no agency or department of the United States Government has officially sanctioned any of these views and opinions.

Acknowledgments

I thank my wife, Lucy for her lifelong support. She has endured many career changes and the stress these bring, countless separations and having to handle everything when I travel, and too many long nights with me working late. Without her enduring love, steady support and salient advice over the years, I would not have had success or the opportunity to become a Fellow in the Senior Service College.

I want to thank my son, Andy. He has inspired me from the day we learned he was going to be part of our family. Despite being severely dyslexic, he has always demonstrated a can-do attitude and not used dyslexia as an excuse, instead committing to overcoming the barrier and resolving to succeed and excel.

Additionally, I want to thank Brian Sabourin, Jack VanKirk, and Jim Baxter for giving me the opportunity to come and work for Program Executive Office (PEO), Aviation as a contractor in support of the Aviation Systems Project Office. Their friendship, patience, and guidance in helping me learn Army acquisition and the PEO Aviation programs will never be forgotten.

I am also grateful to the leadership of MG(R) Tim Crosby, Rusty Weiger, and Layne Merritt for their continued mentoring and for providing me the opportunities to serve in a variety of roles within PEO Aviation and especially in my last role as the Chief Information Officer, CIO/G6.

Table of Contents

List of Tables and Figures

Abstract

A 15-year-old hacked into the National Aeronautics and Space Administration (NASA) and acquired source code that runs the International Space Station, causing NASA to shut down its network for three weeks (Wilson, 2000). In a sanctioned event, a 14-year-old demonstrated he could hack into an automobile's computer and start a car. He used $15 worth of electronics he purchased the day before and built his successful hack that evening (Brantly, 2017). These are single actors with extraordinary talent, but extrapolate this to a federally supported army of talented individuals, and the capabilities they possess become exponentially frightening. China is rumored to have several divisions of cyber-hackers, and Russia places emphasis on computer and math education and is known for developing some of the most famous malware in existence (Kumar, 2015; Blau, 2004; Krebs, 2017).

This study explores the use of Modular Open Systems Approach (MOSA) as an open architecture approach to develop and maintain cyber-resilient weapon systems. Historically, program managers have chosen to use a single-source, proprietary solution, which has been demonstrated to be a slow, high-cost tactic for maintaining a weapon system (SEI Podcast Series, 2015). Slow and expensive are not attributes conducive to maintaining a cyber-resilient system. In the world of cybersecurity, with constantly improving cyber attacks, it is mandatory to respond rapidly to threats from a multitude of adversarial types, including nation states, terrorists, and rogue individuals.

The Department of Defense and the Army recognize the need to address both issues and have produced guidance for program managers to obtain cybersecurity certifications, such as an Authority to Operate (ATO), for systems and to employ an open system architecture for weapon systems where practical. However, obtaining an ATO is a point-in-time event that grows

obsolete before the weapon is fielded, due to both the rapid advances in the threat technology as well as hackers' ever-changing tactics.

The point and time ATO issue creates a dichotomy in the program's cost, schedule, and performance mandates. The expense and time for addressing a constantly moving cyber target must be weighed against the other development and maintenance requirements for the system. In addition to the cost and schedule concerns, we cannot ignore the element of performance. Employing improved cybersecurity can negatively impact a system's performance in two ways. First, improperly designed security can degrade performance or applying restrictive access procedures can make rapid employment of the system impossible. Second, expensive upgrades to combat the cyber threat negatively impact the ability to spend funding on innovative improvements to the system. Given that "the military has a difficult task of reducing costs while continuing to innovate," it is essential to employ an open system approach which provides for more alternatives leading to cost, schedule, and innovation benefits (Haynes, 2013, p. 1).

Adoption of MOSA has been slow due to a lack of education on the value this approach brings to the program manager (Moore, 2016). This trend must change to provide more resilient systems to our warfighters and to allow for more rapid patching and updates for weapons, giving them a stronger cyber threat defense posture. Army leadership must make program managers place focus on cybersecurity for weapon systems through the integration of open systems architecture to provide the flexibility needed to maintain system survivability against cyber threats throughout the system's entire lifecycle.

Introduction

Background

In its report to the House Armed Services Subcommittee on Tactical Air and Land Forces, the Government Accountability Office (GAO) stated, “Traditionally, DOD has acquired proprietary systems, which are costly to upgrade and limit opportunities for competition” (GAO, 2013, p. 2). Unfortunately, another disadvantage in maintaining a long-held, vendor-locked approach for weapon system development and sustainment: a lack of cyber resiliency, which directly impacts the system’s ability to survive.

In a 2013 Report to the Under Secretary of Defense for Acquisition, Logistics and Technology (USD AL&T), the Defense Science Board (DSB) concluded, “While DoD takes great care to secure the use and operation of the ‘hardware’ of its weapon systems, these security practices have not kept up with the cyber adversary tactics and capabilities” (Gosler, Von Thaer, 2013, p. 1). The *Washington Post* reported that, as early as 1996, the GAO warned that adversaries had taken over some defense systems (Gregg, 2017). The article also pulled a quote from the GAO report, which said, “Cyber attacks can target any weapon subsystem that is dependent on software, potentially leading to an inability to complete military missions or even loss of life” (Gregg, 2017, para. 15). This ability to target specific systems is a growing trend in the hacker community (Bradley, 2018, May 4).

Furthermore, according to a 2018 report the GAO submitted to Congress on Weapon Systems Cybersecurity from 2012 to 2017:

> DoD testers routinely found mission critical cyber vulnerabilities in nearly all weapon systems that were under development. Using relatively simple tools and techniques, testers were able to take control of these systems and largely operate

undetected. In some cases, system operators were unable to effectively respond to the hacks. (Chaplain et al., 2018, p. 21)

This illustrates the critical nature of placing an emphasis on cybersecurity, as adversaries are using much more sophisticated tools and techniques to gain control of systems. If simple tools and techniques readily succeed in infiltrating our systems, there is little hope for stopping the more sophisticated approaches. In a report first released in 2002 and updated several times between then and 2015, Carnegie Mellon University illustrated (Figure 1) that while the growth in the sophistication of the types of attacks has increased, these attacks have been developed by a smaller number of experienced hackers, and the overall knowledge level of the average hacker has decreased (Such, Gagliardi, & Woody, 2015). This increased sophistication is coupled with the ease of use of the necessary tools, meaning that potential hackers no longer need to be as

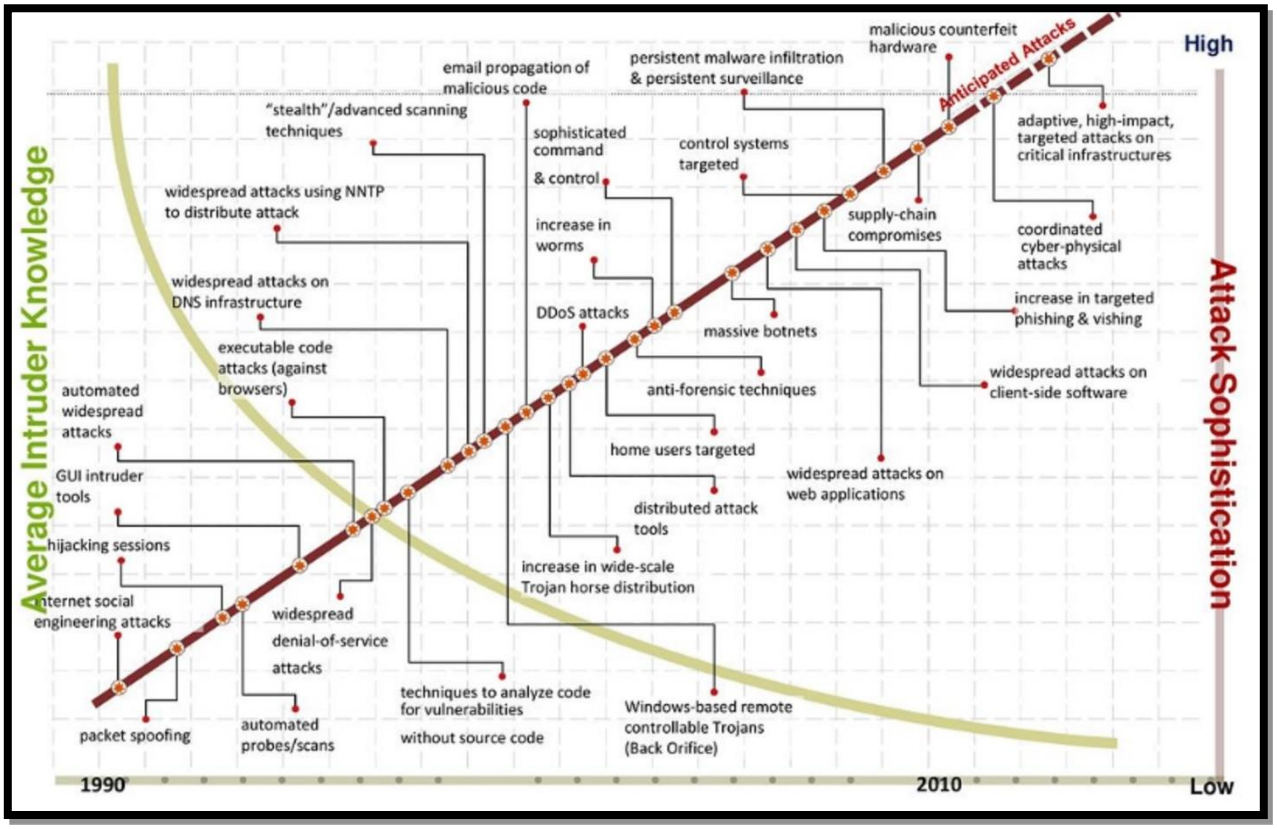


Figure 1. Attack sophistication versus average intruder knowledge (Cooke, 2013).

knowledgeable about the details of building a successful hack. Those with the advanced knowledge frequently build the capability and provide it freely to all via the Internet. With simple point-and-click user interface technology, inexperienced hackers are now making use of highly sophisticated tools to launch cyber attacks on our systems.

Capability enabled by software and a requirement to interoperate with other systems dominates development time and costs for most weapon systems. To demonstrate, the advanced capabilities demand sophisticated and complex software in commercial and military aircraft, which translates to exponential growth in the number of lines of source code needed to support these requirements (Figure) (Simi, n.d.). This increase in complexity thus forces the costs and time necessary to develop and ultimately maintain the software to surge at an equal pace (Cochran, 2001). Additionally, these requirements introduce more complicated cybersecurity

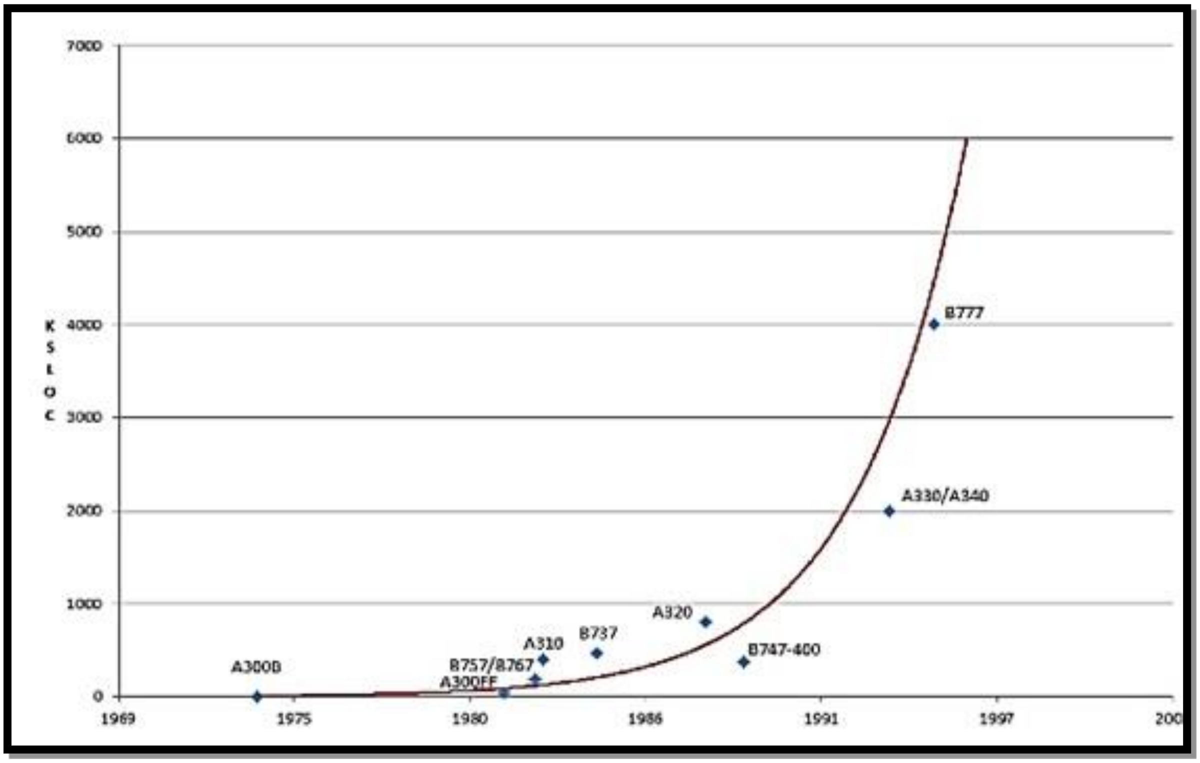


Figure 2. The growth in software complexity from 1969 to 1997 (Simi, n.d.).

demands on program managers and their teams to keep these systems secure in the face of increased cyber threats from peer or near-peer adversaries.

Software has become a significant component of all DoD weapon systems and network communications. The capabilities software delivers will continue to grow to provide our warfighters with the tactical advantage to dominate our adversaries. This growth introduces a concern that the very adversaries these systems are developed to defeat will incapacitate or degrade them. The increase in the number of countries, organizations, and individuals with capabilities to infiltrate virtually any system with computing technology means every system—commercial or military—is susceptible to a cyber attack. An analysis shared by Statista (2018) shows there were 157 data breaches in 2005; that number grew to just under 1,600 in 2017

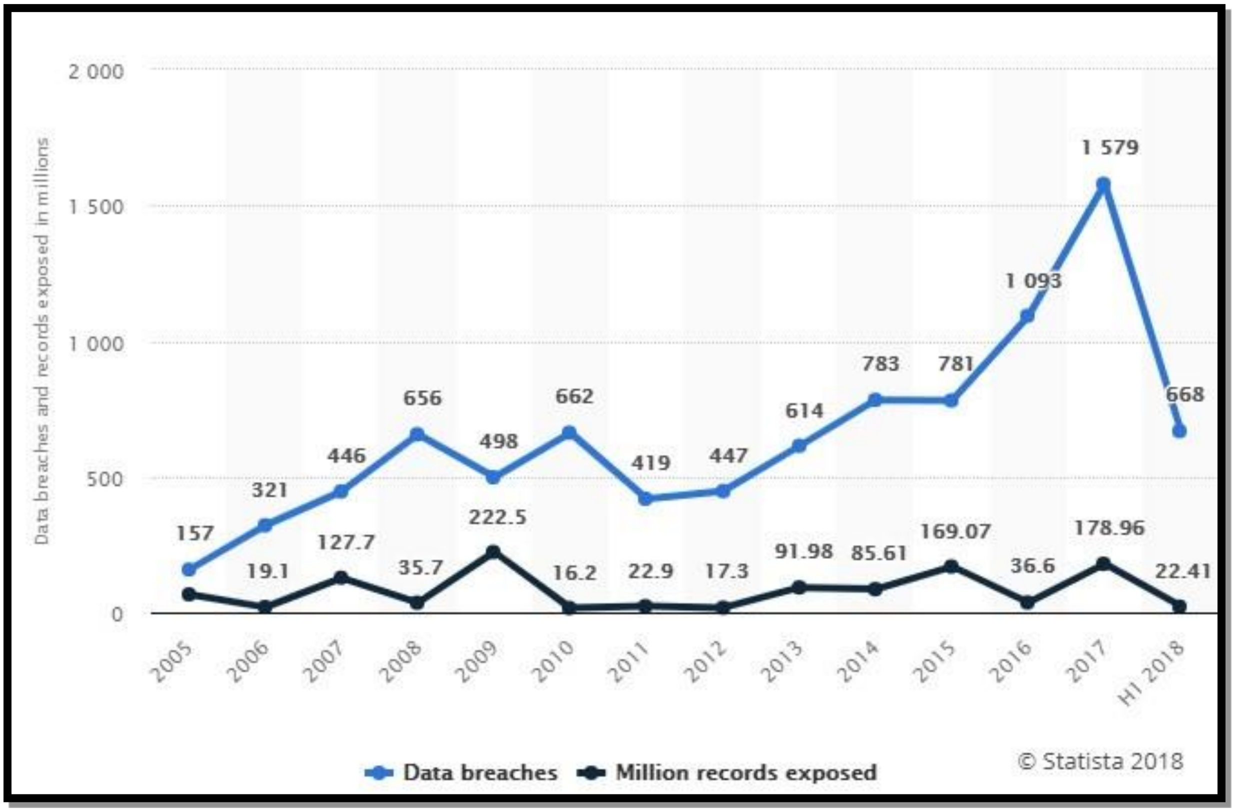


Figure 3. Data breaches from 2005 to 2018 (Statista, 2018).

(Figure 3). These breaches impacted organizations within government and industry and caused billions of dollars in damages, lost time, and lost revenue.

In a study of 2017 cyber attacks, the Online Trust Alliance identified three steps to improve security and reduce the risk of having data stolen from the network: regularly updating the software, blocking fake email and training users (Seals, 2018). Each of the three recommendations improve the security posture; however, the software updates pose the greater impact on the cost of a system and are the most difficult for weapon system program managers to implement at the pace needed to keep their systems secure.

As stated earlier, the staggering number of lines of source code coupled with the need to keep the systems updated to address the swiftly changing cyber threats will put a significant cost burden on program managers. The rapidly growing and changing threats require these weapon systems to exist in a perpetual state of vulnerability, given the length of time needed to develop, test, and implement any patches, updates, or enhancements to thwart the enemy’s cyber assaults (Secureworks, 2017; Sobers 2019).

Definitions

This paper will use terms that may be unfamiliar or may be interpreted differently by the reader. There are numerous definitions for each of these terms, which may differ based on the context or point of view of the source. To ensure consistency in understanding throughout this paper, the following definitions are provided:

- **Architecture**: The specifications of a system designed under multifaceted, set principles defining structure, organization, and relationships of the components.
- **Cyber attack**: An attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm (Merriam-Webster, n.d.).

- **Cyber Survivability Attributes** (Lamolinara, 2018)**:**
    - **Prevent**: Design requirements that protect weapon system's functions from most likely and greatest risk cyber threats. This includes:
        - CSA 01 – Control Access,
        - CSA 02 – Reduce Cyber Detectability,
        - CSA 03 – Secure Transmissions and Communications,
        - CSA 04 – Protect Information and Exploitation,
        - CSA 05 – Partition and Ensure Critical Functions at Mission Completion Performance Levels, and
        - CSA 06 – Minimize and Harden Cyber Attack Surfaces.
    - **Mitigate**: Design requirements that detect and respond to cyber-attacks, enabling weapon systems functions resiliency to complete the mission. This includes:
        - CSA 07 – Baseline & Monitor Systems, and Detect Anomalies, and
        - CSA 08 – Manage System Performance if Degraded by Cyber Events.
    - **Recover**: Design requirements that ensure minimum cyber capability available to recover from cyber attack and enable weapon system to quickly restore full functionality. This includes:
        - CSA 09 – Recover System Capabilities.
    - **All 3 KPP Pillars** are touched by the final attribute:
        - CSA 10 – Actively Manage System's Configuration to Counter Vulnerabilities
- **Cybersecurity**: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire

communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation (DoD CIO, 2014, March 14).

- **Modular Open System Approach (MOSA)**: An integrated business and technical strategy for competitive and affordable acquisition and sustainment of a new or legacy system, or a component within a system, over the entire system life cycle (ODASD, 2017).
- **Open Architecture**: A system in which the specifications are made public in order to encourage third-party vendors to develop add-on products.
- **Open System**: A system in which the components and protocols conform to standards independent of a single supplier.
- **Open System Architecture (OSA)**: An architecture in which the interrelationships of the components are defined by interface standards, and the architectural principles and guidelines are consistent with an open systems approach (Oberndorf & Sledge, 2010, p. 23).
- **Proprietary (Closed) Architecture:** A system not available to outside software developers or manufacturers. Closed architecture prevents outside companies from developing products for such a system (Held, 2006).
- **System Architecture**: The fundamental organization of a system, embodied by its components, their relationships to each other and the environment, and the principles governing its design and evolution (MITRE, 2015).
- **System Survivability Key Performance Parameter (SS KPP):**

> Intended to ensure the system maintains its critical capabilities under applicable threat environments. The SS KPP may include reducing a system’s likelihood of being engaged by hostile fire, through attributes such as speed, maneuverability, detectability, and countermeasures; reducing the system’s vulnerability if hit by hostile fire, through attributes such as armor and redundancy of critical components; enabling operation in degraded electro-magnetic, space, or cyber environments; and allowing the system to survive and continue to operate in or after exposure to a Chemical, Biological, Radiological and Nuclear (CBRN) environment, if required. In System of System (SoS) approaches, it may also include resiliency attributes pertaining to the ability of the broader architecture to complete the mission, despite the loss of individual systems (Department of Defense, 2015).

Problem Statement

The United States is the largest target of cyber attacks in the world, the next two countries, India and South Korea, combined make up less than half of the number of attacks the United States experiences (Significant Cyber Incidents, 2018). The Department of Homeland Security (DHS) reported a significant increase in cyber incidents against U.S. critical infrastructure in 2015 (Meola, 2016; Jordan & Boudreau, 2013). In another report released in 2017, the GAO discussed the increased reliance on computer-based technologies and how the Department of Defense’s (DoD) limited—but emerging—knowledge of how to protect these systems from a cyber-perspective raises concern from leadership (Government Accountability Office, 2017). The same report highlights the chief challenge in providing cybersecurity for DoD is the services’ weapon systems dependency on software for providing critical capabilities and communicating over networks.

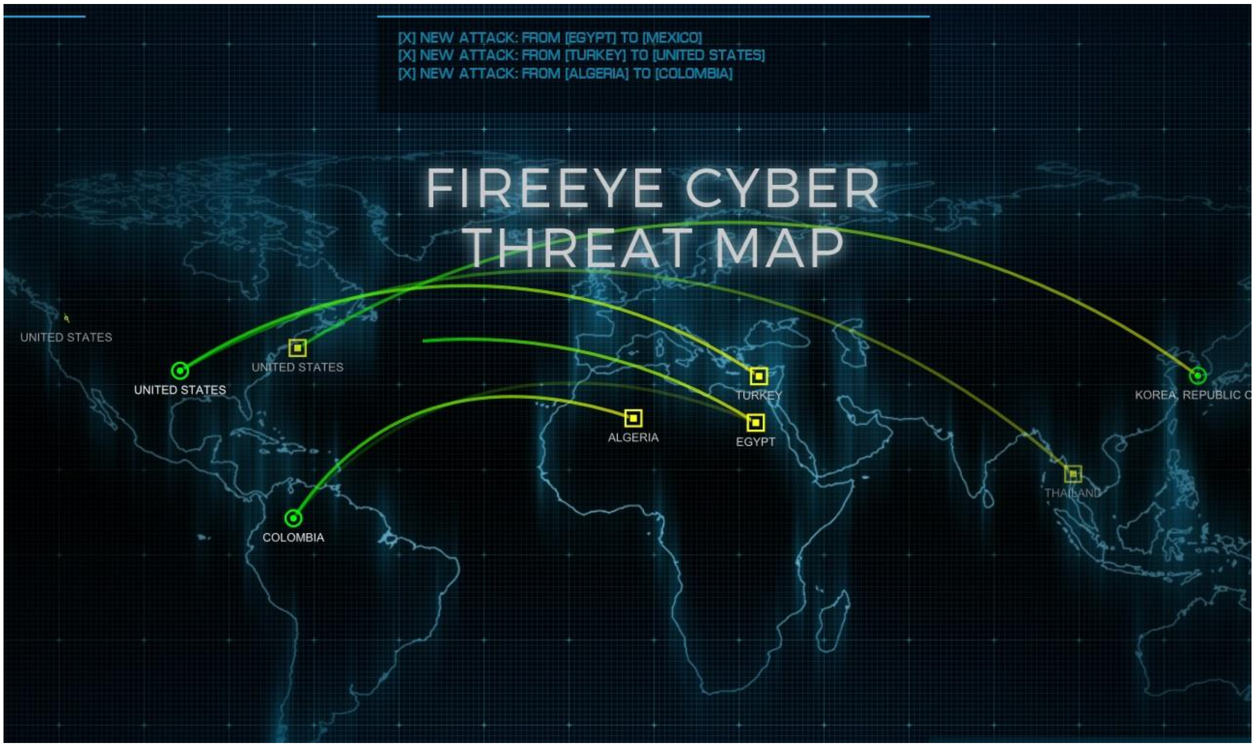

[X] NEW ATTACK: FROM [EGYPT] TO [MEXICO]
[X] NEW ATTACK: FROM [TURKEY] TO [UNITED STATES]
[X] NEW ATTACK: FROM [ALGERIA] TO [COLOMBIA]
FIREEYE CYBER
THREAT MAP
UNITED STATES
UNITED STATES
UNITED STATES
TURKEY
EGYPT
ALGERIA
COLOMBIA
THAILAND
KOREA, REPUBLIC O

Figure 4. Increase in threats from all parts of the world (Fireeye, 2018).

Given that the typical approach to developing weapon systems is often based on the proprietary architecture of the supplier, follow-on upgrades or enhancements almost always entail exercising the same proprietary path (SEI Podcast Series, 2015). So, the question becomes: How can an open systems approach be applied to address cyber survivability to rapidly mitigate and counter cyber threats to weapon platforms, allowing them to continue the fight after absorbing a cyber-incident?

Program managers, engineers, testers, and users must be aware of the cybersecurity implications for their systems and actively contribute to the engineering design considerations and Tactics, Techniques, and Procedures (TTP) to be able to defend against and fight through cyber attacks.

Purpose of the Project

This paper will examine the value open systems architecture provides in developing weapon systems to be more cyber-resilient. Assuming open systems architecture benefits the entire lifecycle of any system, the intended focus of this study will be narrowed to how this approach impacts the adaptability—thus, survivability—of the weapon system in a cyber-contested environment. The significance of this topic is grounded in the exponential rise in the level of sophistication and escalating frequency of cyber-attacks on all DoD systems. The combination of threats and slow progress in addressing cybersecurity make our weapon systems increasingly susceptible to successful breaches. Cyber resiliency must be a key design consideration to maintain a weapon system's effective operational status in much the same manner as maintenance or reliability are considered when designing traditional military weapons and vehicles such as an aircraft, tank, truck, or missile.

Significance of Research

The Honorable Frank Kendall, Under Secretary of Defense for Acquisition, Logistics, and Technology (USD(AL&T)) recognized the importance of securing weapon systems and frequently made statements directly addressing the critical nature of cybersecurity. In an email on the subject he declared, “The threat is pervasive and dynamic—it isn’t going away and will never be fully defeated,” (Gregg, 2017, para. 20). In his statement to cyber team members at the U.S. Navy's Space and Naval Warfare Systems Command (SPAWAR), he stated, “The overall focus of BBP 3.0 is the overriding concern that U.S. technological superiority is at risk” (Borland, 2016, para. 9). The Better Buying Power (BBP) 3.0 initiatives are focused on the chief areas of concern or interest from the DoD leadership, which makes this statement more significant. Given the prevailing concerns outlined by DoD, this paper is significant and timely, as there is a reluctance to include the added design elements needed to develop an increased cybersecurity posture of a weapon system (Schmidt & Sledge, 2016).

Until recently, for most weapon systems, there has been little emphasis placed upon cybersecurity. This fact is illustrated in a recent GAO report highlighting that the cybersecurity test results for a five-year span were so poor that “DoD likely has an entire generation of systems that were designed and built without adequately considering cybersecurity,” (Chaplain et al, 2018, p. 18). This lack of cyber consideration is probable, due to a lack of specific direction in Operation Requirements Documents (ORD) or Capability Development Documents (CDD), under which most current programs operate (Murray, n.d., p. 5). This oversight has recently changed with specific guidance for cybersecurity in several documents across the DoD and services. For example, in 2015 the Joint Chiefs of Staff (JCS) updated their Joint Capabilities

Integration and Development System (JCIDS) to include new a Key Performance Parameter (KPP), System Survivability, of which a key element is cyber survivability.

As depicted in Figure 5, adding more cybersecurity features is a more complicated and costly effort upon discovering a vulnerability. Another key consideration is that program funding decisions and funding priorities are made very early in a programs lifecycle. Failure to plan for and resource cybersecurity early in the life cycle means that cybersecurity will not be a funding priority later. Lack of funding causes further delays in testing beyond the time needed to implement fixes, as an additional cyber scan and analysis is needed when attempting to obtain an Authority to Operate (ATO) (Gregg, 2018). Applying fixes to issues late make the corrections much more difficult and drive up the price of the system (Stecklein, 2004). The rise in cost is exacerbated by the fact that the bulk of our weapon systems are developed by original equipment manufacturers (OEM) and suppliers using proprietary or closed solutions. These systems do not provide the program manager the flexibility to explore cybersecurity considerations outside of the OEM or their subcontractors. This typically means there are limited options, which center on

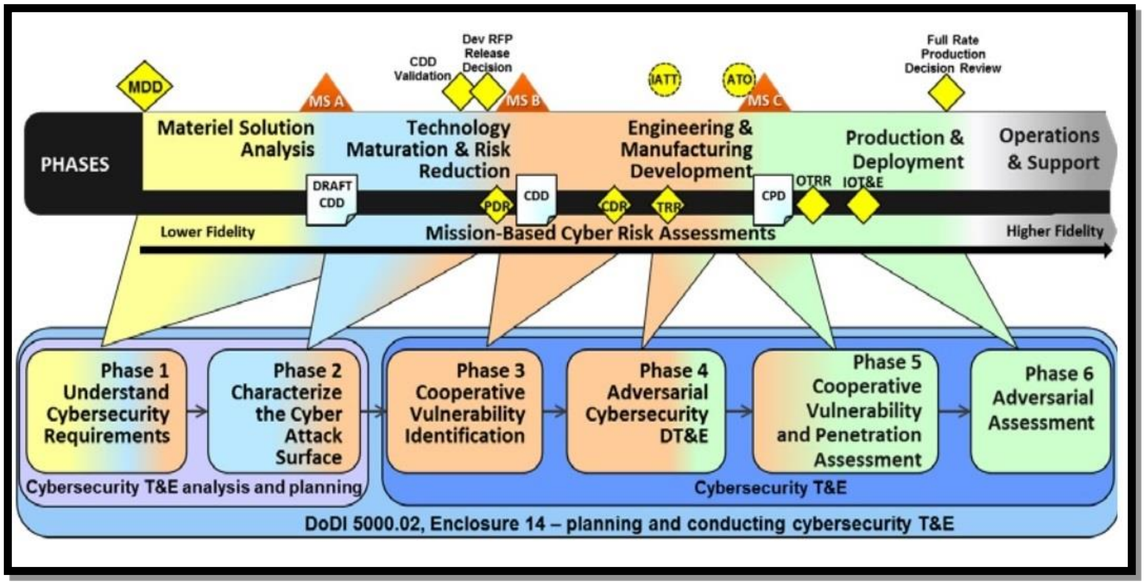

MDD
CDD Validation
Dev RFP Release Decision
MS A
MS B
IATT
ATO
MS C
Full Rate Production Decision Review
PHASES
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Production & Deployment
Operations & Support
DRAFT CDD
PDR
CDD
CDR
TRR
CPD
OTRR
IOT&E
Lower Fidelity
Mission-Based Cyber Risk Assessments
Higher Fidelity
Phase 1 Understand Cybersecurity Requirements
Phase 2 Characterize the Cyber Attack Surface
Phase 3 Cooperative Vulnerability Identification
Phase 4 Adversarial Cybersecurity DT&E
Phase 5 Cooperative Vulnerability and Penetration Assessment
Phase 6 Adversarial Assessment
Cybersecurity T&E analysis and planning
Cybersecurity T&E
DoDI 5000.02, Enclosure 14 – planning and conducting cybersecurity T&E

Figure 5. Cybersecurity in the acquisition lifecycle (Department of Defense, 2018, p. 7).

the original provider or one of its vendors, when attempting to bolt on expensive and time-consuming solutions. Once implemented, these solutions can prove to be ineffective, given the rapid rate of change of cyber-attack approaches and tools.

While conducting their study on weapon systems' cybersecurity, the GAO reported to the Senate that "this failure to address weapon systems cybersecurity sooner will have long-lasting effects on the department." (Chaplain et al., 2018, p. 18). Newer systems with high-level cyber protections also feel a ripple effect, as each system must interface and interoperate with the older systems that have easy-to-exploit vulnerabilities. Once an adversary successfully infiltrates an older system, the connectivity with newer systems translates to an increased risk of intrusion or malware infection for the newer systems via these connections.

Our weapons systems do not operate in isolation, as each requires interoperability or, at a minimum, communication with other systems to provide or receive data critical to the successful operation of the system or to provide the maximum benefit of the capability. The significance this plays in cybersecurity is immeasurable, since the quantity, stealth, and degree of effectiveness of malware, such as worms that can traverse over network links and infect virtually any type of computing device, is growing. Interconnectivity and interoperability are both a requirement and a curse for our systems. The Army needs to connect with our team, including other services and coalition partners, but this requirement correspondingly provides the necessary connectivity for our adversaries to potentially exploit our system's vulnerabilities from numerous avenues. The DoD needs both interconnectivity and interoperability to win on the battlefield, so protecting these capabilities rises proportionally in importance with the precipitous increase in threats (Lacdan, 2018). This means more than system engineers designing and developing cyber-hardened systems. The finance and contracting contributors must have a basic awareness of the importance of cybersecurity and adequately fund and contract for including work necessary to complete design and development of more survivable systems. The operators of the weapon systems must be keenly aware of the threats and be trained so they are able to respond to attacks, allowing their system to continue to operate and stay in the fight. The people aspect of a cyber-resilient system cannot be ignored, and the DoD is working to develop the offensive and defensive cyber soldiers that will be able to respond to cyber incidents (Sholtis, 2017).

The world witnessed the destructive capability of Stuxnet, a zero-day worm with stealth capability, bring down the nuclear capacity of Iran (Zetter, 2017; Ranger, 2018). This worm—and there are many others—traveled to its target location over time via several networks and systems. There is no reason to believe a similar event has not been launched or is at least planned for a helicopter, tank, missile, or command and control system within the DoD inventory. Should this type of attack be launched, it will require the combined capabilities of the system's cyber defense and the operators to thwart the attack and keep the system mission capable. To do this, engineers must design the system to meet the Cyber Survivability Attributes, and the Army must educate the operators to understand these attributes and train them to execute the TTPs for cyber incident response.

Recent use of cyber warfare by Russia against Georgia, Crimea, and Ukraine illustrate that the strategic use of denial of service of important infrastructure, such as electrical and cellular services, is going to be the normal approach for engagement. Destroying or significantly degrading the ability to exchange data and communicate is as important as or more important than targeting tanks and missiles with conventional firepower (Park, Summers, & Walstrom, 2017).

Research Questions

This paper will address the following questions to assist the reader in understanding MOSA, cybersecurity threats, and the value of designing systems with open architectures. It will bring realization that aggressively treating cybersecurity as a design consideration significantly reduces risk. The key is to develop the best strategies for mitigation of emerging cyber threats and to minimize the negative consequences if a cyber-attack is successful.

1. What constitutes an open system architecture (OSA)?
2. Are there added costs and time associated with developing a system using OSA?
3. Does the use of OSA add to the complexity of the system development?
4. Can a legacy system developed using proprietary architectures incorporate an open systems component?
5. What is cybersecurity for weapon systems?
6. How does incorporation of cyber defense impact system cost, schedule, and performance?
7. How does an OSA help improve the cybersecurity posture of a system?
8. How much OSA is enough? How can this best be measured?

Objectives and Outcomes

There are mandates and guidance from the DoD and the Department of the Army for including an open systems approach where feasible (Murray, 2012). The Office of the Deputy Assistant Secretary of Defense (ODASD) (2017) identifies the primary benefits for systems incorporating an open systems approach:

- Increasing competition,
- Facilitating technology refresh,
- Innovating,
- Saving money, and
- Enhancing interoperability.

Leadership has updated existing guidance and created new guidance to address the need for cybersecurity for all DoD systems. The overarching benefit of following this guidance is a staunch resistance to our adversaries' cyber-attacks, making our systems more cyber-survivable.

The objective of this research is to determine the value of implementing an open systems architecture when designing and developing weapons systems to make them more cyber resilient. An OSA is a foundation for future efforts, as we are required to maintain a strong capacity for meeting the system survivability KPP. To do this requires combating relentlessly changing cyber threats while keeping costs low and reducing development timelines.

The discussion will illustrate the value an open system architecture has on creating a weapons system with reduced lifecycle costs, lower integration risk, and diminished susceptibility to obsolescence. Program managers that initiate design with an open systems approach will find they are in an improved position to address the need to patch, modify, or enhance their weapon system when the cyber environment necessitates action (Guertin, 2018; Zimmerman, 2015).

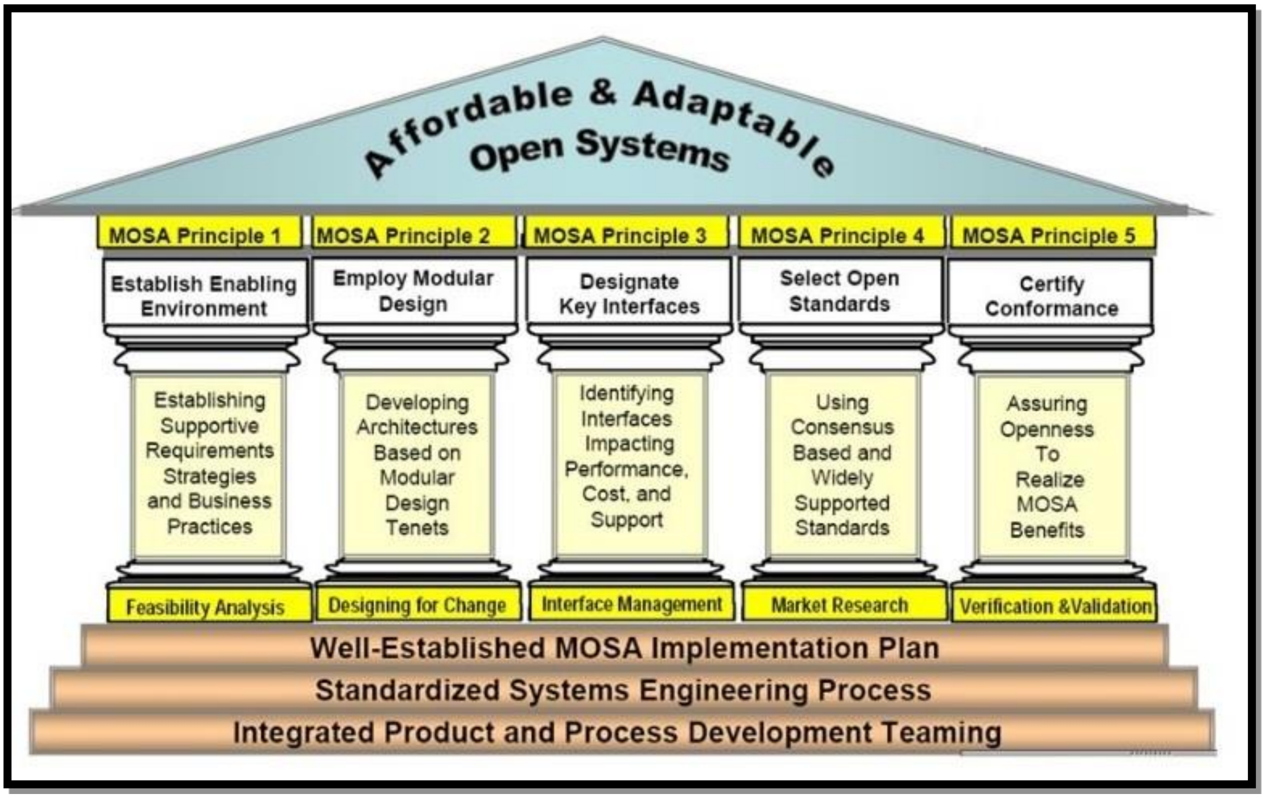

Affordable & Adaptable
Open Systems
MOSA Principle 1
MOSA Principle 2
MOSA Principle 3
MOSA Principle 4
MOSA Principle 5
Establish Enabling Environment
Employ Modular Design
Designate Key Interfaces
Select Open Standards
Certify Conformance
Establishing Supportive Requirements Strategies and Business Practices
Developing Architectures Based on Modular Design Tenets
Identifying Interfaces Impacting Performance, Cost, and Support
Using Consensus Based and Widely Supported Standards
Assuring Openness To Realize MOSA Benefits
Feasibility Analysis
Designing for Change
Interface Management
Market Research
Verification &Validation
Well-Established MOSA Implementation Plan
Standardized Systems Engineering Process
Integrated Product and Process Development Teaming

Figure 6. The pillars of affordable and adaptable open systems: MOSA Principles (Defense Acquisition University, n.d., p. 88).

Applying the MOSA principles of modular open systems (Figure 6), specifically principles two and four, provide the ability to incorporate change to meet the demanding and rapid changes necessary to improve overall system survivability from a cybersecurity perspective (Zimmerman, 2015). Without any significant events, there remains a requirement under the Risk Management Framework (RMF) to scan the system annually as part of maintaining a valid ATO (Air Force LCMC, 2018). Any findings during the annual scan must be mitigated, which may require system modifications or updates to TTPs. By complying with the open systems architecture guidance, the program can maintain compliance with the cybersecurity requirement with lower costs and reduced time to field impacts compared to a proprietary system (Air Force LCMC, 2018).

Literature Review

Guidance

The concept of using a MOSA — or modular, open approach — to developing systems has reached the DoD and is codified in several directives and instructions. The Department of Defense Directive (DoDD) 5000.01 Change 2, August 31, 2018 – "The Defense Acquisition System" and the Department of Defense Instruction (DoDI) 5000.02, August 10, 2017 – "Operation of the Defense Acquisition System" provide clear directions to consider the use of MOSA to design and develop systems. The 5000.01 language directs programs to use a modular, open-systems approach where feasible, while the 5000.02 further defines this to include the subsystem level, allowing programs to complete upgrades and employ multiple sourcing.

Adopting MOSA standards gives the program managers several benefits (Rutkowski, 2019). First, an open architecture with independent modules allows for completing components for enhancements or improved cybersecurity posture. Second, the program office is not required to update the entire system when a component needs to be replaced. Next, as requirements change to meet mission, cyber, or obsolescence needs, the system can be configured more easily and can accept innovative assets rapidly. Another benefit is cost savings, as the modular, open system accepts components from any supplier and can reuse technology developed under the same open standards. Finally, as more systems incorporate open systems architecture and share technology across weapon systems, the level of interoperability increases. This is significant in that open systems can more rapidly address needed changes to weapon systems to provide enhancements, fixes, and changes needed to meet constant cyber threats (Rutkowski, 2019; Zimmerman, 2018).

The increased concern over cyber vulnerabilities in all DoD systems led the JCS update the Manual for the Operation of JCIDS to include a requirement for all programs to meet cyber survivability as a KPP (Department of Defense, 2015). This effectively ensures cybersecurity is mandated for all DoD systems.

These and other guidance are clearly referenced in several memos from Honorable Frank Kendall (USD(AL&T)). In a recent memo to the Chairman of the Defense Science Board, the Honorable Kendall points out that military systems are susceptible to cyber attacks on the heavily used Non-classified Internet Protocol Router (NIPR) network (Kendall, 2017). The DoD guidance combined with the 2018 DoD Cyber Strategy illustrates that DoD leadership recognizes the value of employing an open systems approach to developing systems as well as the need for strong cybersecurity.

Army regulations mimic much of the direction the DoD provides. The Department of the Army, CIO/G6 (2017) recently published Lead*ers Information Assurance / Cybersecurity Handbook*, which points out, “Army regulations, policies and guidance provide the Army imperatives authority, responsibility and accountability necessary to promote a culture that is risk aware and complies with practices that minimize vulnerabilities to Army networks, systems and information” (p. 2). The CIO/G6 admonishes Army leaders to “ensure that your organization remains committed to practices that protect Army networks, systems and information” (Department of Defense, 2017, p. 2).

The Army recognizes that every connected system has some level of vulnerability and our adversaries have sophisticated hacking tools but can make use of low-cost technology and other tools to attack our systems (Department of the Army, 2007). Because our weapon systems are an attractive target for our adversaries, the Army has a requirement to test and certify all systems prior to granting permission for their connection to an Army network (Department of the Army, 2013). However, simply passing through the RMF process and addressing the current risks to the satisfaction of the Authorizing Official (AO) is not enough to ensure the most effective security possible for the system (Department of Defense, 2015). The controls within RMF lack focus on meeting mission risk and operational resiliency weapon systems must have to be effective in the face of a cyber attack. The users must understand the threat and, through training, be able to respond to incidents in a manner that keeps the system operational. Another level of incident response is to report attacks and the resulting impacts, so the cyber professionals and system engineers can address the vulnerability and design fixes. These can be materiel or TTPs that they implement to thwart future attacks of the type detected (Department of Army, CIO/G6, 2017).

Acknowledging the importance of the initial design in relation to building a cyber-resilient system, the 2018 *National Cyber Strategy* demands we "promote foundational engineering practices to reduce systemic fragility and develop designs that degrade and recover effectively when successfully attacked" (The United States of America, 2018, p. 16). The 2018 DoD Cyber Strategy echoes the significance of maintaining a collaborative approach between services and industry partners to "strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages" (Department of Defense, 2018, p. 1). The DoD cyber strategy’s guidance to accelerate development, innovate, and use existing commercial capabilities modified for military use are best addressed using an open systems architecture in weapon systems (Department of Defense, 2018, p. 4; Dattathreya, Cummings, & Sharafi, 2018). The past approach of vendor-specific, proprietary systems has clearly demonstrated that acceleration and integrating closed systems are not complementary requirements (Dattathreya, Cummings, & Sharafi, 2018).

The RMF for DoD Information Technology requires all systems to obtain an ATO prior to receiving approval to field (Department of Defense, CIO, 2014, March 12). The RMF is designed to identify the security controls a system must address based on its security profile (Jackson, 2018). The RMF process focuses on addressing risks and deciding whether a system should be fielded and used, based upon the mission requirements weighed against the risks identified in security scans and testing. This process recognizes the inherent dangers of cyber-vulnerabilities, and the annual scans enforce a constant review and analysis of the risks. However, this is only one piece of the total package necessary to secure our systems. Everyone who touches the system, from requirements personnel to the operators and their leaders, must understand the importance of cybersecurity in general and the specifics for their system to be effective in reducing the threats upon the system's ability to operate.

Open Systems

Open systems architecture combines well-defined interfaces with a modular approach to developing a system to allow for reduced life-cycle cost and time required for upgrades, system expansion, or maintenance support (Norton, 2015; Tokar, 2017). Adopting OSA creates a competitive environment for systems to build and maintain a system over its useful life. With upward of 70% of a system's cost occurring in the sustainment phase, the benefit of reduced cost and schedule are primary drivers pushing DoD leadership to encourage weapon system program managers to advance designs to OSA (Doubenspeck, 2016). The open architecture enables more vendors to participate in the acquisition process and provide innovative solutions to a system, ensuring its ability to accept enhancements, combat obsolescence, and robustly defend against evolving threats (Department of Defense, 2013). The resulting increased competition is a considerable benefit for creating a cyber-resilient system, as program managers have alternatives to provide needed adjustments when enhancing their systems and addressing obsolescence or cyber vulnerabilities.

The characteristics common to capabilities developed under an open systems architecture include many of the requirements program managers have sought for their platforms or systems. A well-developed open architecture will support interoperability, reusability, maintainability, and scalability (ODASD, 2017). Each of these performance parameters is important for a successful program and are more achievable with an open architecture. The unlocked specifications this architecture provides equates to opening the door for multiple vendors to realistically compete for technology insertions. A larger pool of potential vendors creates competition, which leads to innovation and more aggressive pricing—a phenomenon that has been demonstrated in several commercial industries, including the computer hardware and software markets (GAO, 2013). The defined interfaces mean that integration complexity is greatly reduced, leading to reusability, but is also a significant enabler for new capabilities to be developed and integrated as well (Tokar, 2017).

Despite the demonstrated advantages of an OSA development approach, many program managers are more comfortable relying upon the single OEM or vendor’s proprietary approach for building systems (Schmidt & Sledge, 2016). There is an element of value in long-term relationships with trusted OEM sources when supporting the weapon systems they helped to design and build. Unfortunately, attempting to maintain a proprietary architecture in the face of cyber threats leaves our systems in a highly susceptible state and at risk of becoming ineffective, or worse, causing catastrophic results for our warfighters (Bradley, 2018; Hayes, 2017). Systems are no longer able to rely upon taking the “security through obscurity” approach as the primary means to avoid cyber threats. The days of hoping secret design architectures or that a hacker will not be able to find vulnerabilities in the system have long disappeared (Bradley, 2018, December 12). This way of thinking is no match for today’s increasingly wily cyber adversary (Keeney, 2018).

There are several reasons for this reluctance to adopt OSA. In many cases, the primary reason programs may be hesitant to migrate is due to the sheer volume of software they have already acquired for their systems. In addition, the government workforce may be trailing industry in understanding open architecture and the value this method brings to a development approach (Serbu, 2013). When it comes to building open architectures, industry and government must join forces in recognizing the value this approach can bring to each side. Bringing the workforce on board is likely difficult, as many developers that built and now maintain these systems hold a “not invented here” condition that is prevalent in industry and within the services’ program offices (Schmidt, 2014).

Another roadblock for adopting open systems is the misconception that open makes the system more vulnerable to cyber-attacks (Irwin, 2018). The foundation of this fear is rooted in the confusion in terminology between open source and open systems. An open source software offering is typically a no-cost executable with the original source code made available should the user wish to modify the application for specific needs (Midrack, 2018). In most instances, users with little to no due diligence download only the executable from the Internet. While there are vast numbers of legitimate providers of open source software, the lack of research can result in installing software infected with malware (Irwin, 2018). An open system is a design approach involving the technical architecture under which a system is designed using a standards-based foundation coupled with the business element of contracting for or supplying the capabilities developed using this approach. Designing a system with open architectures and interfaces does not mean a supplier must reveal the "secret sauce" of a capability like we see in open source software (Pellerin, 2014). To illustrate, the algorithms used in a navigation system do not need to be an element of the open portions of a product. An open source solution can apply the open system approach, but it is not mandatory to use this approach to be classified as an open source software application.

Understanding open systems is not common knowledge for everyone involved in developing requirements, designing solutions, contracting for the development, or managing the program. To embrace an approach, it must be well understood to alleviate concerns or misconceptions about the impacts the architecture may have on the system. Education is essential for everyone involved in the system on open systems to the level necessary for their roles in the process (Sledge, 2015). There should be no mysteries or misconceptions inhibiting the adoption of an open systems approach as a viable means to achieve interoperability, adaptability, and robustness of a weapon system.

When program managers accept OSA, they are typically looking to reduce costs and risk to their programs (Schmidt & Sledge, 2016). PMs quickly realize this is important beyond the development phase, as illustrated in the reduction in costs and time needed to maintain a system over a long duration. Maintenance involves hardware and software, as both elements will require attention as a system is used over time. In the case of software, an obsolete operating system may need to be replaced. Since the early stages of computing, many hardware companies have followed traditional proprietary architectures by directly coupling the operating system to the hardware (Shaffer, 2015). This practice was common to gain efficiencies in processing, given the limited resources available in early hardware and software components. Conversely, a proprietary architecture is not conducive to rapid change, since a modification to update an operating system can become a major project that is both costly and time-consuming while keeping the system tied to a single vendor (Fisher, 2014). However, an open, modular approach incorporating decoupling of hardware and software greatly reduces the effort for changing an operating system, as there are no required changes—or at most, smaller modifications—to software, and hardware components need no work done on them (Malekzadeh, 2014). Adoption of OSA is imperative for DoD program managers to move their systems away from stove-piped methodologies to provide warfighting capability (Sledge, 2015).

The services are working with industry and academia to develop architectures and standards to support this decoupling strategy (Serbu, 2019; Wong, 2013). The Future Airborne Capability Environment (FACE^{TM}) and the Sensor Open Systems Architecture (SOSA^{TM}) are consortia made up of members from the defense industry, academia, as well as the Army, Air Force, and Navy, focusing on a technical and business standards-based open systems approach to developing capabilities for the warfighter. In addition, organizations like the Aviation Development Directorate (ADD) of the U.S. Army Combat Capabilities Development Command (CCDC) Aviation and Missile Center (AvMC) are using these open systems approaches to reduce the need to repeat development efforts for similar capabilities across aviation platforms (Wigginton & Jacobs, 2018). This means related reduction in integration and testing events further reducing implementation timelines. Such a benefit translates into a system having improved response times to cyber threats as a primary avenue for successful breach of a system through software vulnerabilities. Open systems allow for more rapid adaptability, allowing the employment of patches or upgrades to combat the threats identified since the last release of the software (Tokar, 2017). This is critical, since, historically, once a vulnerability has been discovered, the number of attacks on a system rapidly increases as the knowledge of the exploitability spreads (Arbaugh, Fithen, & McHugh, 2000). In fact, the intrusion attempts will increase for a time after a patch has been released (Figure 7) until the hacker community learns through discovery that the vulnerability has been mitigated. Proprietary systems limit the resources available to address issues and are more likely to be limited in the ability to employ emerging technologies without significant time and expense (Norton, 2015).

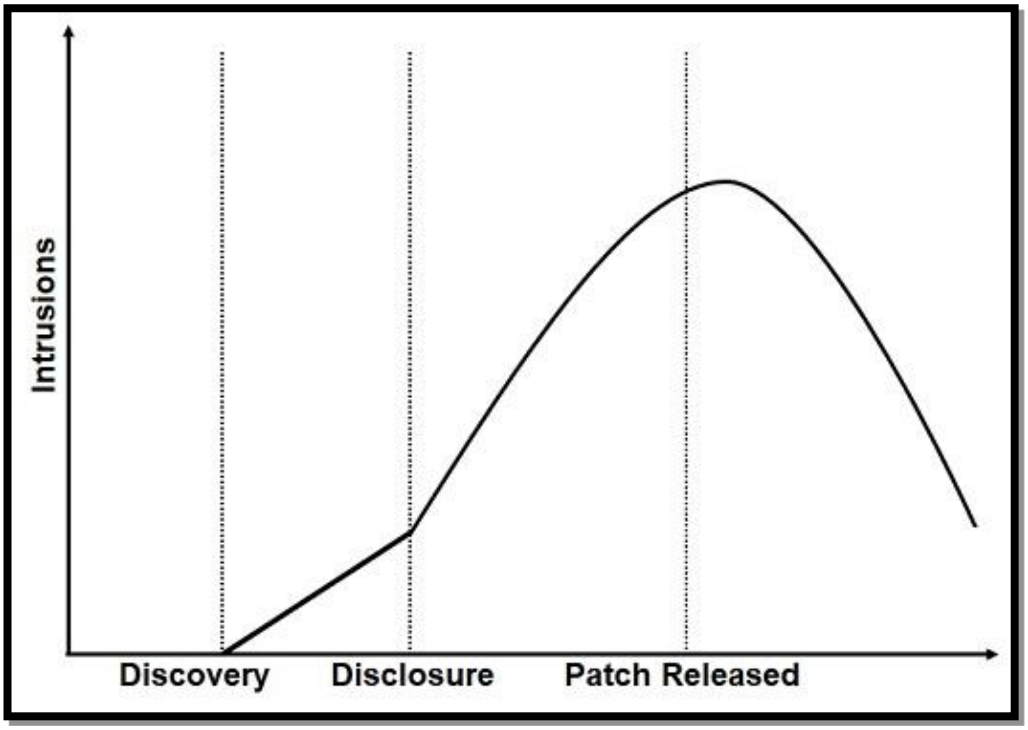


Figure 7. Intrusion rates increase with the discovery of vulnerability (Arbaugh, Fithen, & McHugh, 2000).

The exclusive relationship a proprietary solution creates translates to a higher potential of new technology insertions essential to address issues that are not likely to happen in a timeframe that helps the program manager keep pace with the demands that growing cyber threats have introduced (Davis, 2018). Commercial providers have adopted the open systems approach in a wide range of industries, which means the DoD program managers must move in this direction if they are going to comply with the DoD Cyber Strategy's guidance to make use of Commercial off the Shelf (COTS) capabilities as the base and optimize them for use on weapon systems (Department of Defense, 2018, September 18).

While the focus of the value proposition for open systems is centered on reducing costs and the time to field these systems, one should note that other benefits of an open architecture include reduced risk for obsolescence and improved cybersecurity (Manning, 2017). Proprietary software capabilities built upon tightly coupled hardware limits the refresh and growth potential to the boundaries within the hardware. Similarly, proprietary hardware solutions are limited to the innovation schedule and abilities of the original provider. The DoD Under Secretary of Defense (ATL), Kendall identifies numerous initiatives in his BBP 3.0; one is to "strengthen cybersecurity throughout the product lifecycle," and another is to "use Modular Open Systems Approach (MOSA) to stimulate innovation" (Department of Defense, Under Secretary of Defense, 2015, p. 2). Verifiable system interfaces developed to a common set of well-defined standards make using MOSA approach for designing and developing systems possible, thus supporting more rapid modifications that the system will need over its lifecycle (Wigginton & Jacobs, 2018).

Current proprietary architectures are especially vulnerable to exploitation and are difficult to modify when changing threats jeopardize the survivability of the system (Schmidt, 2013). This holds true when we examine the largest provider of operating system and office automation software in the world: Microsoft. The model Microsoft employs is a closed system, and it experiences continued growth in the number of vulnerabilities hackers exploit each year (Loeb, 2018). The issue is the number of eyes Microsoft can pay to design, develop, and test its software products. To help reduce the errors in its software, the company uses early releases to a limited community of users to alpha and beta test major releases (Vijay, 2018). While this method is an effective approach, it is difficult to detect everything that might generate an exploitable condition, so Microsoft issues patches on a routine basis to combat the known defects discovered since the last patch (Fisher, 2019). Frequent patching at the level of a commercial, proprietary software product is not possible in proprietary weapon systems under contracts to specific vendors.

In cases where program managers have significant resources tied to a proprietary solution, it is important to understand that OSA remains a viable consideration. Despite having proprietary origins, there are options available for incorporating capabilities designed under the OSA concepts (Serbu, 2013). The first step is that the program manager must recognize the need for taking a hard look at proprietary systems and find creative ways to add open interface enhancements for integration. For example, the Air Force added open interfaces to its Distributed Common Ground System (DCGS) using an approach called “sidecar” (Serbu, 2013). Taking this method and applying it to the proprietary DCGS enables developers from the “outside” to use the interface definitions to build capabilities and integrate them with DCGS’ core application.

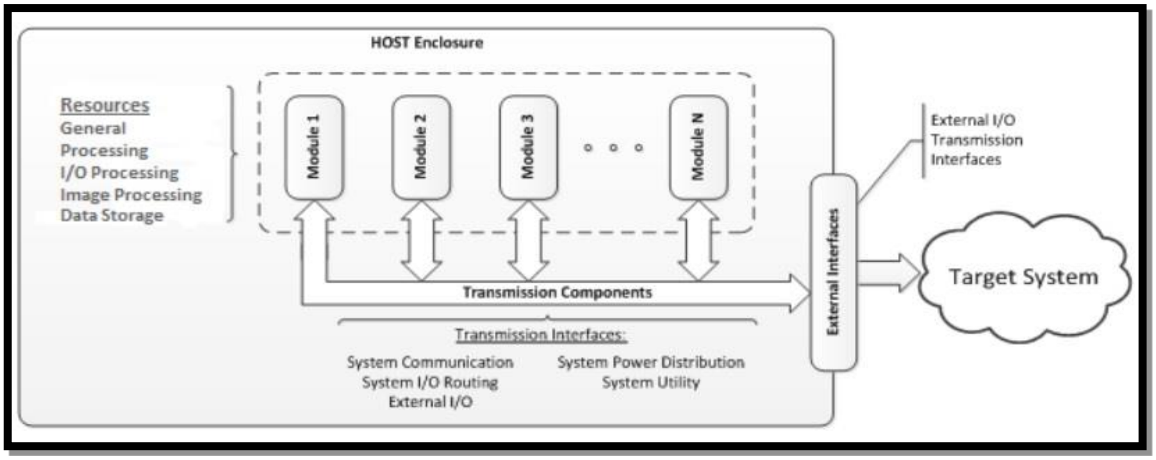


Figure 8. Example HOST component categories.

As previously mentioned, there are numerous efforts where the defense industry, academia, and the DoD Services have joined forces to develop open, standards-based guidelines for both hardware and software architectures. The Hardware Open Systems Technology (HOST) led by the Naval Air Systems Command (NAVAIR) establishes a set of hardware standards that, when followed, provide opportunities for any hardware vendor to compete to provide a component (Warshawsky, 2015). There are four components defined under the HOST standard: modules, enclosures, external interfaces, and transmission (Figure 8). Briefly, the module component defines independent hardware management and monitoring as well as data exchange standards. The enclosure establishes processing and storage resources. The external and transmission components set the interface standards for communication for external and internal I/O respectively (Collier, 2017). The Navy, Army, and Air Force each have active development and Small Business Innovation Research (SBIR) efforts for systems that are adopting the HOST standard for a variety of systems.

Another significant standards community, the FACE^{TM} Consortium, focuses on providing a standards-based, open, modular approach to developing avionics software. To meet this goal, the consortium has followed the guiding principles within Open Architecture (OA), Integrated

Modular Avionics (IMA), and MOSA to develop a standards-based approach for reusable and

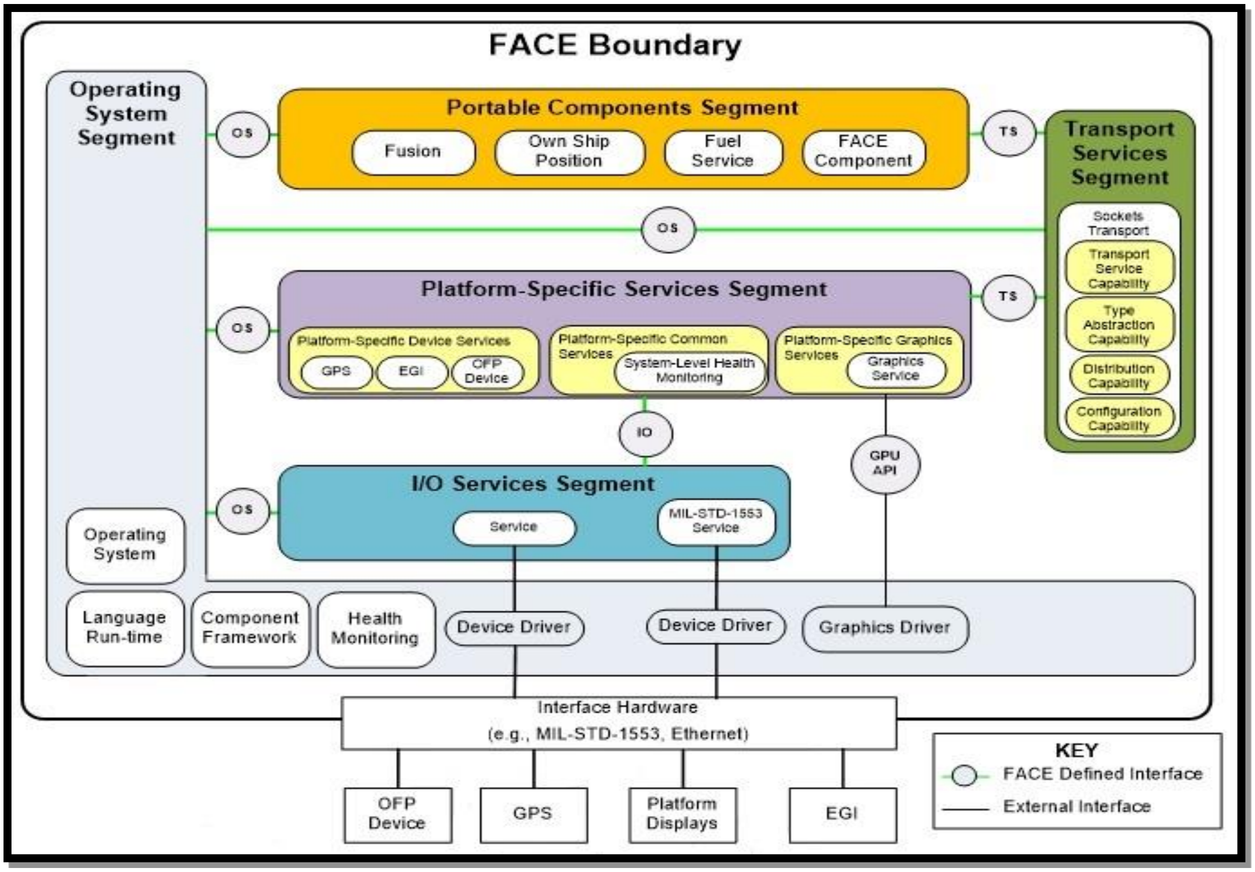


Figure 9. An example of FACE^{TM} architectural segments (Open Group, 2017).

portable avionics software. By defining architectural segments (Figure 9) and abstracting the hardware layer, the FACE^{TM} technical standard can be applied to all aviation platforms (Open Group, 2017).

The underlying infrastructure is developed to be conformant to the MOSA standard, which means any capability developed to the FACE^{TM} standard is compliant with the DoD directive to use MOSA where practical (Open Group, 2017).

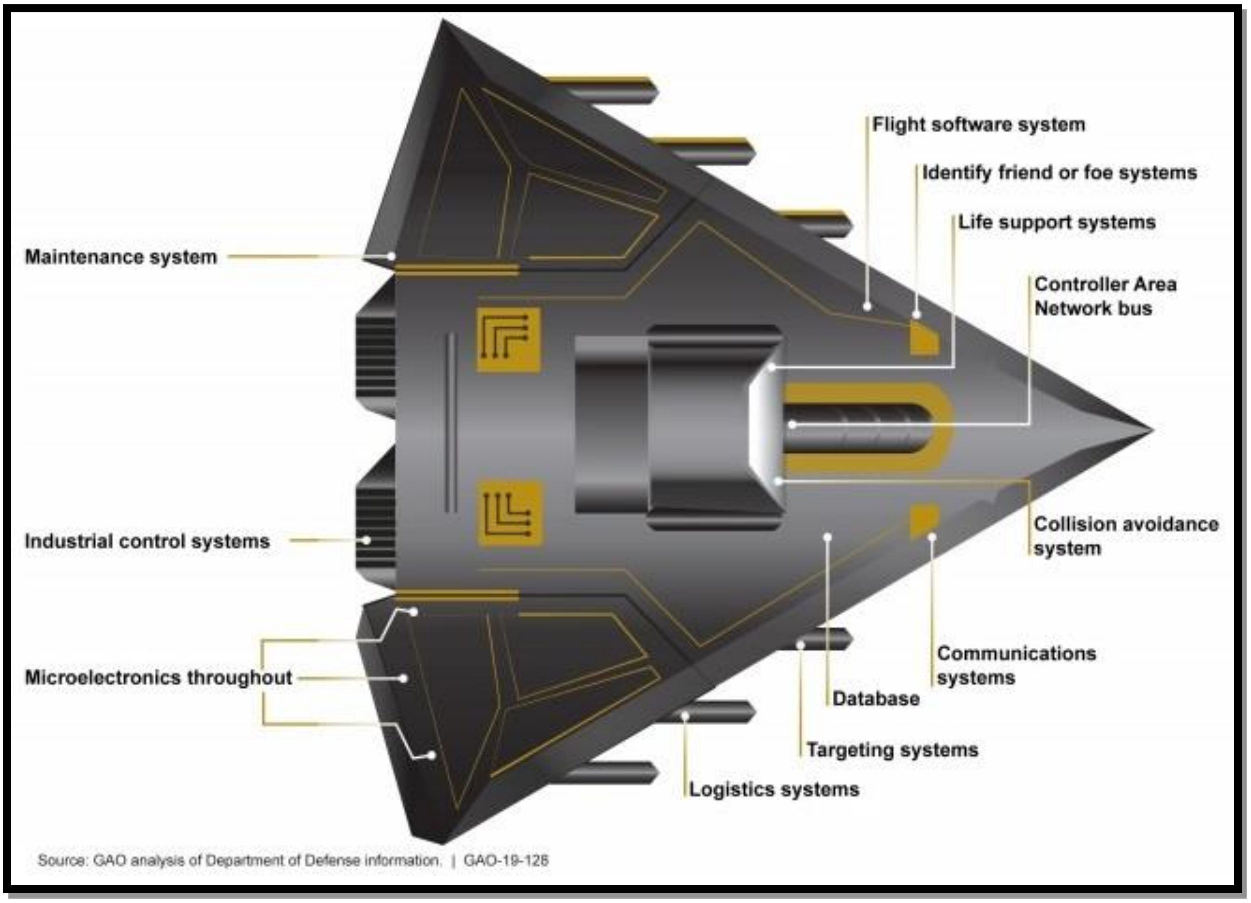
Cybersecurity

The very nature of cybersecurity is mysterious to most people, including those charged with developing and maintaining the DoD weapon systems (Dolan, 2016; Mazanec, 2015). A recent statement from the DoD Defense Science Board highlights this fact, saying, “The United

States cannot be confident that critical IT systems can be defended from a well-resourced cyber adversary," (Mazanec, 2015, p 194). Understanding cybersecurity is important to be aware that in the cyber domain, an adversary can be one of our traditional near peer nation-states, such as Russia or China; rogue nation states, including North Korea and Iran; terrorist groups; or a 14-year-old with $15 worth of equipment purchased at an electronics store and an evening's worth of time (Brantly, 2017).

Computer and weapon systems are more complex, and the methods used to build them are equal in complexity, leading to costs that are escalating to levels that are becoming prohibitive. If this trend, continues it will eventually price the services out of their ability to provide technology to their users. The DoD recognizes the need to put a focus on developing offensive and defensive cyber capabilities more rapidly, pointing to it as one of the department's strategic lines of effort in the 2018 DoD Cyber Strategy. Specifically, the strategy's first line of effort reads, "Build a more lethal joint force" (Department of Defense, 2018, p.4). Each of the four components of the building a more lethal force line of effort illustrates the critical nature of speed, innovation, improving technology, and using existing commercial capability. The strategy emphasizes accelerated development and denotes qualities such as "adaptable" and "scalable" as key for providing flexibility to commanders. The innovative aspect directly speaks to the need to be agile to keep up with "rapidly evolving threats and technologies in cyberspace" (Department of Defense, 2018, p. 4). Agility is only obtainable through the use of an open systems approach for new systems and implementing changes in existing systems.

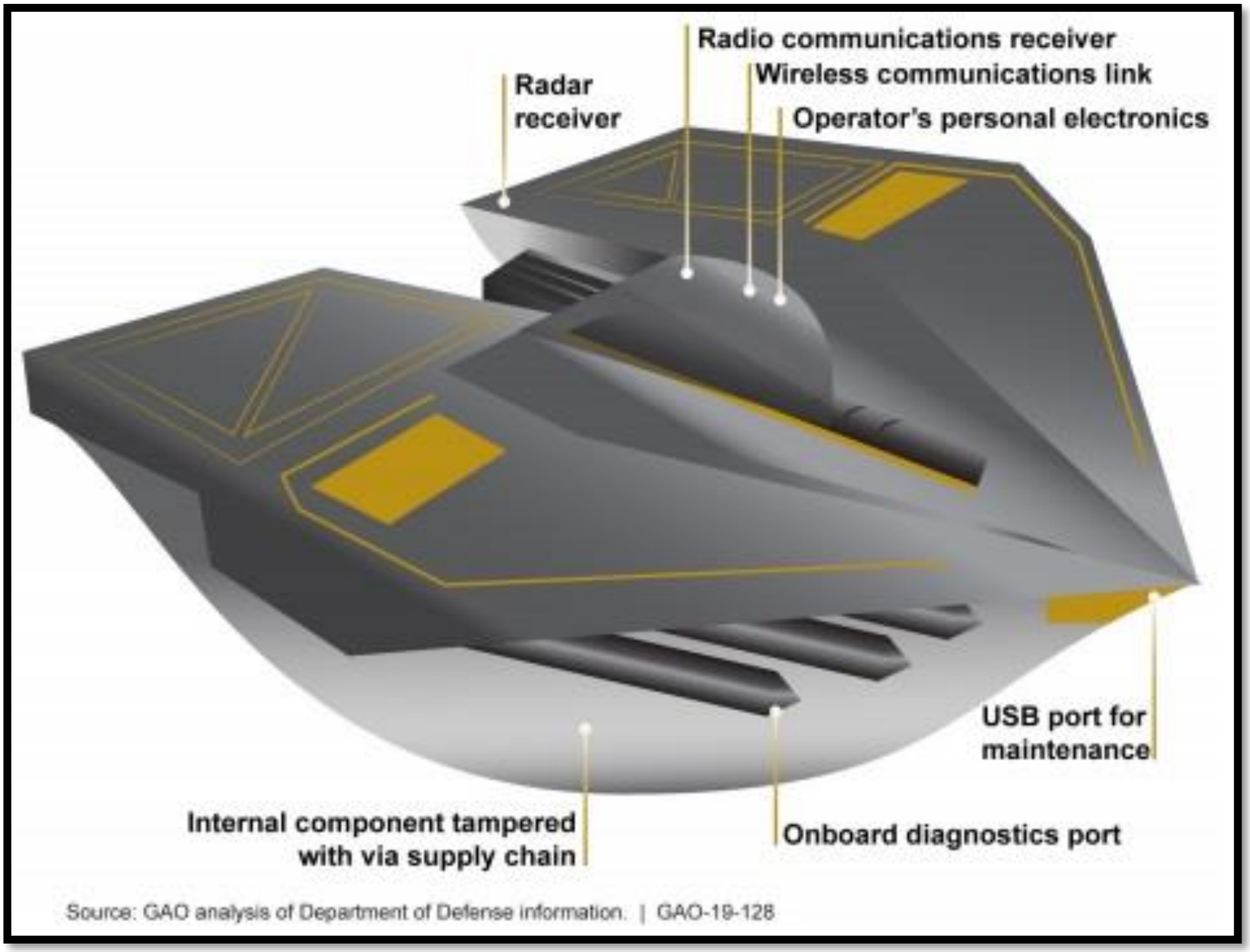
On a positive note, the level of integration of hardware, software, and communication has tightly joined our systems to provide capability far beyond those of only a decade ago. This rapid growth has introduced technical issues in maintaining the cybersecurity posture of these complicated systems (DiMase, Collier, Heffner, & Linkov, 2015). Nevertheless, increasing complexity has led to software growth within the weapon systems. However, despite the best testing efforts each program office and DoD have established, there are still exploitable vulnerabilities in every system (Hawkins, 2018).


Flight software system
Identify friend or foe systems
Life support systems
Maintenance system
Controller Area Network bus
Industrial control systems
Collision avoidance system
Communications systems
Microelectronics throughout
Database
Targeting systems
Logistics systems

Source: GAO analysis of Department of Defense information. | GAO-19-128

Figure 10. An illustration of a fictitious weapon system's embedded software and information technology (Chaplain et al., 2018).

A recent GAO report to the Committee on Armed Services of the U.S. Senate described the potential cyber-attack surface of a weapon system to clarify the extent of the cybersecurity surface (Chaplain et al., 2018). While the system, illustrated in Figure 10, is fictitious, it provides an eye-opening view of the problem space. Each of the software and hardware components identified represents a target of opportunity that potentially opens access to the other embedded elements of the system should an adversary successfully infiltrate it. A second illustration further enhances this issue by depicting potential points of entry into a weapon system, as shown in Figure 11 (Chaplain et al., 2018). A common misconception many program offices have is that the systems they are developing are somewhat immune to the common threats of cyber-attacks that desktops and enterprise networks are subject to because their systems and weapon systems are protected by gates, guns, and guards that limit access. For program managers of mobile weapons systems, this false sense of security is expanded because they believe that moving is another obstacle to an enemy combatant's or terrorist hacker's successful cyber strike. The GAO report shows these interfaces to explain the multiple points of entry requiring defense, which should gain the attention of anyone responsible for architecture, design, development, or testing these systems (Chaplain et al., 2018). In addition to the


Radio communications receiver
Wireless communications link
Radar receiver
Operator's personal electronics
USB port for maintenance
Internal component tampered with via supply chain
Onboard diagnostics port

Source: GAO analysis of Department of Defense information. | GAO-19-128

Figure 11. An illustration of a fictitious weapon system's interfaces (Chapain et al., 2018).

communications elements of these systems, there are the ports used to plug into systems to perform maintenance or download data that onboard systems capture. These plugged-in systems typically are used on other networks, which provide opportunities for malware to be introduced to the weapon systems when authorized personnel connect them for maintenance or other activities (Chaplain et al., 2018).

The increased dependency on complex software introduces a higher potential for software defects (Huda et al., 2018). Defects of varying degree will exist despite the best efforts of developers and testers. Coupling new systems with the vulnerabilities in the older, outdated systems commonly in use across the DoD means there are significant contributors to potential cyber vulnerabilities (Chaplain et al., 2018). Older systems with outdated operating systems make attractive targets, since their vulnerabilities are well-known and likely not patched or updated in any manner due to diminished support from vendors (Irwin, 2018; Lindros, 2016).

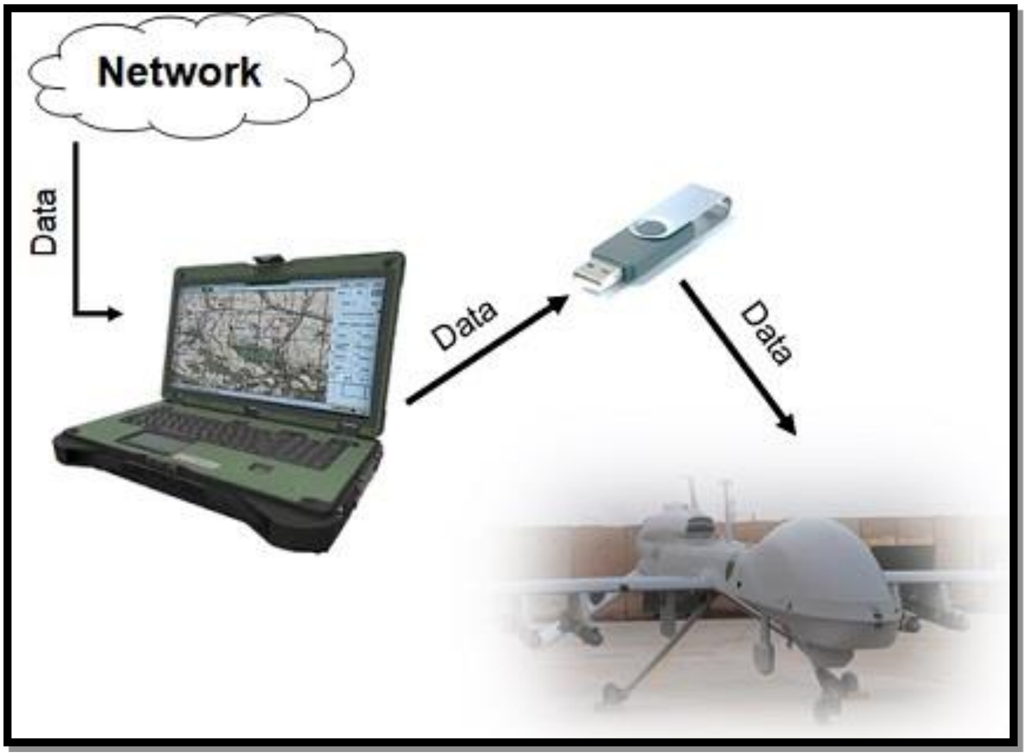


Figure 12. The flow of data via manual transfer using (a potentially compromised) USB drive (Carlson, 2018).

Because newer systems are required to interoperate with other systems, old or new, all interconnected systems now share common weaknesses. These weaknesses are not limited to networked systems, as many weapon systems also require Universal Serial Bus (USB) ports to allow plug-in devices to connect (Chaplain et al., 2018). The connectivity of these USB devices shares similar risks to networked systems, since their source of data comes from a networked computer and then is transferred via a manual process to connect to the weapon system (*Figure 12*).

Hackers discover and quickly exploit software flaws such as communication shortcomings found in such protocols as Secure Sockets Layer (SSL) or User Datagram Protocol (UDP). In many cases, hackers make these exploits freely available to anyone who wishes to download them or sometimes sell them to organizations or nation-states in cases of zero-day exploits that are not known (Perlroth & Sanger, 2013). Most industry experts estimate that there are 15 to 50 software defects, typically referred to as bugs, per 1000 source lines of software code (SLOC) (Anderson, 2018). Reports indicate that the Android operating system has numbers as low as five bugs per 1000 SLOC (Buley, 2010). Microsoft estimates that it finds about 10 to 20 defects per 1000 SLOC during testing but that its production versions end up with less than one defect per 1000 lines. The true number depends on the complexity of the software and experience levels of the developers.

Now, take for example the Air Force’s F-35 Lightning II Fighter Jet, which has over 8 million lines of complex code supporting a variety of avionics critical to the flight and functionality of the aircraft (Heusel, 2017). Using the lower number of defects estimated for production software at Microsoft means that users can expect about 8,000 defects of varying levels. Some of those defects translate to vulnerabilities that may be exploited by a hacker. This can cause the F-35 to be non-operational or might be disastrous if the exploit is able to touch flight controls or other critical avionics. However, implementing an open architecture system development approach like FACE^{TM} introduces the potential to reuse software from similar systems. This goal is not often mentioned, but if used, it can mean using code that has been tested, used, and updated with improved code containing fewer defects, thus reducing the probable vulnerabilities available for a hacker to exploit.

The cyber threats are not exclusively focused on software, given there have been exploits discovered in central processing units. The Meltdown and Spectre exploits take advantage of hardware defects for widely used Intel and Advanced Micro Devices (AMD) microprocessors (Fritze & Schiller-Wurster, 2018). One can mitigate hardware exploits through software or firmware updates or hardware replacements. Threats or successful exploits of this nature, however, are not limited to computers, servers, and smartphones, since these microprocessors are integral components in our jets, missiles, and other weapon systems.

In addition to software and central processing unit (CPU) exploits, there are known breaches to industrial control systems using programmable logic controllers (PLC). This illustrates that malware can move from one type of technology to another. For instance, the Stuxnet worm is purported to have been developed over several years and employed against Windows-based computers with an eventual target of a Siemens’ PLC used by nuclear centrifuges (Zetter, 2017). The Stuxnet worm used network and USB drives to traverse systems until it was able to recognize a connected PLC for which it was designed to attack (Zetter, 2017). This demonstrates a major concern for our weapon systems, as there are many manufacturers and vendors supplying parts and software that factor into the cybersecurity posture. Converting commercial implementation against PLCs to a focus on military-grade PLCs used on ships or missiles is not complex. While Stuxnet and similar worms work through the PLC programming, they can be detected and subsequently quarantined, but there are still larger concerns with potential rootkit level infections impacting the firmware of the PLC, making them much more difficult to detect (Basnight, Butts, Lopez, & Dube, 2013).

Stuxnet is one of three known malware capabilities that have successfully engaged industrial control systems. The others are ‘Industroyer’ and ‘Triton.’ The former is the first known malware used to successfully attack a power transmission station. The outage lasted about an hour, indicating that hackers can take control and cause more damage (Greenberg, 2017). The third malware attack used ‘Tritan’ to take control of a nuclear safety control system in the Middle East (Xie, 2018).

The DoD defense industry supply chain is as dependent upon networked communications and processing power as we are in government (GAO, 2017). The concern over cyber threats injecting malicious software (malware) to generate hidden liabilities into our systems before we assemble them is not limited to the supply chain for each system. There are recorded instances of DoD program offices undergoing attacks as well (Gorman, Cole, & Dreazen, 2009). Focusing solely on the system in inadequate, since an exploited vulnerability is an open door to other connected organizations, as demonstrated by the attack on Target Stores via a trusted heating, ventilation, and air conditioning (HVAC) vendor (DiMase et al., 2015).

Comments such as, “My system is not information technology like your desktop,” is a common statement in the weapon systems’ community. While correct on the surface, the underlying technologies weapon systems employ make them very much like the technology used on our desktops. In fact, there are many instances of desktop technologies making their way into the weapon systems in use on the battlefield today. Examples include the Joint Battle

Command-Platform (JBC-P), a more traditional software and hardware combination used throughout the Army and Marines (Department of the Army, 2012). The Unmanned Aerial Systems' (UAS) use of the One System Remote Video Terminal (OSRVT), a tablet computer capable of connecting to the aircraft and receiving video, demonstrates another traditional IT-based capability (Garbarino, 2017). The primary control for the UAS is the Ground Control Stations (GCS), which can consist of a laptop or a collection of multiple computer systems housed in shelters (Department of the Army, 2012).

In both the OSRVT and GCS, the cyber vulnerabilities go well beyond the minimal software protection antivirus defenses offer. There are other technical liabilities in the hardware and network communications that are necessary to make the UAS an effective tool for the warfighter (Mansfield, Eveleigh, Holzer, & Sarkani, 2015). The network communication link between the GCS and the UAS in flight is especially prone to such attacks as Global Positioning System (GPS) spoofing or jamming (Rani, Modares, Sriram, Mikulski, & Lewis, 2016). Inexpensive technologies and well-known hacking techniques can provide a low cost of entry for a hacker to develop the capability to intercept the controls from the pilot of the UAS and force it to crash or behave erratically (Ranger, 2018). The GCS to UAS communication is not the only networked weapon system capability impacted by the growth of cyber vulnerabilities. The successes of previous attacks, such as Stuxnet and Tritan, are being used as the foundation for improved, more complex attacks that can be implemented against other systems (Basnight et al., 2013; Ranger, 2018).

These and other weapon systems using commercially available or commercial-like processing and operating system technologies are susceptible to the same exploits as traditional computing devices. For example, there is a large market for zero-day exploits that hackers can modify and develop into cyber weapons to attack an unsuspecting system manufacturer and ultimately infiltrate a weapon system (Thomson, 2018). Given the chief tenant of a zero-day, that the provider or user community is unaware it exists, these exploits can take advantage of software weaknesses and disrupt the use of the system, making it unreliable or rendering it inoperable by disabling or destroying some portion of the system (Zetter, 2017; Thomson, 2018). The potentially serious impacts these exploits can have on a system have led traditional operating system and business capability providers, such as Microsoft and Apple, to offer large payouts to anyone who can identify and provide fixes for vulnerabilities in their products (Perlroth & Sanger, 2013). This is not an approach available to the developers of DoD weapon systems, so another method is required to reduce the risks that zero-day and other exploits introduce.

Increases in demand for integrated capabilities reliant upon data from other systems means we are developing more system-level software components to interface these systems to share data over the network. Couple this with a significant growth in the number of people interested in finding vulnerabilities in software, and you have a formula for increased successful infiltrations (Irwin, 2018; Foale, 2018). Expanding dependence on software in weapon systems opens the door for exploitable weaknesses too numerous to adequately defend. Let’s return to our example of the F-35 Lightning II or Joint Strike Fighter (JSF), which is estimated to have more than eight million lines of code managing everything from communications and flight control to sensor fusion and weapons deployment. Given the number of systems that interface with the F-35, the Air Force should have real concerns about protecting the operational capability of the aircraft (Sprenger, 2018).

Similarly, the Army recently upgraded the vital systems—e.g. the sensors and a software-defined radio known as the Join Tactical Radio System (JTRS)—on its battle tank, the Abrams, to connect it to other systems on the battlefield (South, 2017; Department of the Army, 2012). The software-defined radio capability, coupled with the onboard network for this vehicle, introduces network and software vulnerabilities into the platform. Vulnerabilities are inherent with any IT platform that is required to communicate or process data. The sensors use the computer processing power to integrate sensor and radar data to detect incoming grenades or missiles and initiate countermeasures to protect the soldiers and vehicle (Rempfer, 2018). This data must travel via the integrated network for processing on the computer in real time. Any unwanted interruptions to this process would have severe ramifications, including potential loss of life.

Leadership sees improvement in the cyber capabilities but understands that more needs to be done to overcome the military services' history of slowly advancement due to restrictive policies and processes that remain prevalent in its acquisition cycle. General Raymond A. Thomas III, the Commanding General of the U.S. Special Operations Command, complimented our cyber capability, but he also echoed his concern for the restrictive policies in his "Hot Topics" speech to the attendees of the Association of the U.S. Army's Institute of Land Warfare event (Association of the U.S. Army News Staff, 2017). General Thomas III insisted the speed of decision-making and action "must keep pace with the speed of war" (para. 4).

A cyber-attack on military operations could be more devastating than the effects of traditional weaponry (Ranger, 2018). Recognizing an understanding of cyberspace and the policies needed to address security, offensive and defensive strategy, and handling a crisis initiated by a cyber-attack, the Army fields student teams from West Point to compete in cyber-policy case competitions (Suits, 2018). This is the not the only education-related approach to addressing the growing cybersecurity field. The DoD Cyber Strategy (2018) includes providing the current workforce with training opportunities, growing management skills in the cyber arena, and putting significant effort into primary and secondary education to promote science, technology, engineering, and math (STEM) disciplines.

Cyber resilience

"The rapid pace of change, however, is not something we should seek to slow down; rather, it is something we must embrace" (Alexander, 2013, p. 23). This idea points directly to the need for our weapon systems to be cyber-resilient, which maps cleanly to the Protect, Mitigate, and Recover elements of the Cyber Survivability Attributes that are part of the System Survivability KPP mentioned earlier. Army weapon systems take time to develop, and the security—often basic in nature—put into the systems is already vulnerable to new forms of cyber attack when systems are fielded. Despite significant testing prior to production and fielding, both our adversaries' and other hackers' pace of cyber capabilities puts every weapon system behind the curve in terms of defending against the cyber threats they face (AMRDEC Public Affairs, 2016; DoD, 2018; Vijay, 2018).

To maintain system effectiveness in the event of a cyber attack, the system, coupled with the operator's actions, needs to be able to mitigate the impacts and recover to the level necessary to maintain operations. Responding quickly and decisively to cyber-incident that impacts a subsystem or system is the key for resiliency. Implementing MOSA approach for the system's architecture can segment the critical areas of the system to address the confidentiality, integrity, and availability (CIA) of the physical system in the event of a cyber attack (Sheets, 2018). To complete the total system resiliency, the Army must train the people element with the appropriate TTPs for cyber incident handling and response to keep the system operational in its potentially degraded mode (Honkus, 2015).

According to Xie (2018), on December 14, 2017, there was a little-publicized, successful breach of a nuclear safety control system believed to be located in the Middle East. The attackers, assumed to be members of a nation-state, used malware to gain control of a workstation for the safety control, Xie (2018) noted, but per the design, the system automatically shut down to prevent any damage. While the hackers were successful in taking control of the system, the automatic shutdown thwarted any more illicit activity. However, what we must consider is that the attack did take the system offline, which may have been the attackers' initial desire (Finkle, 2017). This points to a lack of cyber resiliency, as the capability of the system was not available for a period.

Now, translate this example into a weapon system during a battle. The effect of shutting down to avoid damage or unintended results is tantamount to the system being destroyed. The goal of a weapon system incorporated with true cyber resiliency in its design is to minimize the negative impacts of a cyber attack and ideally allow the system to continue to function as intended without fear of damage or malfunctioning.

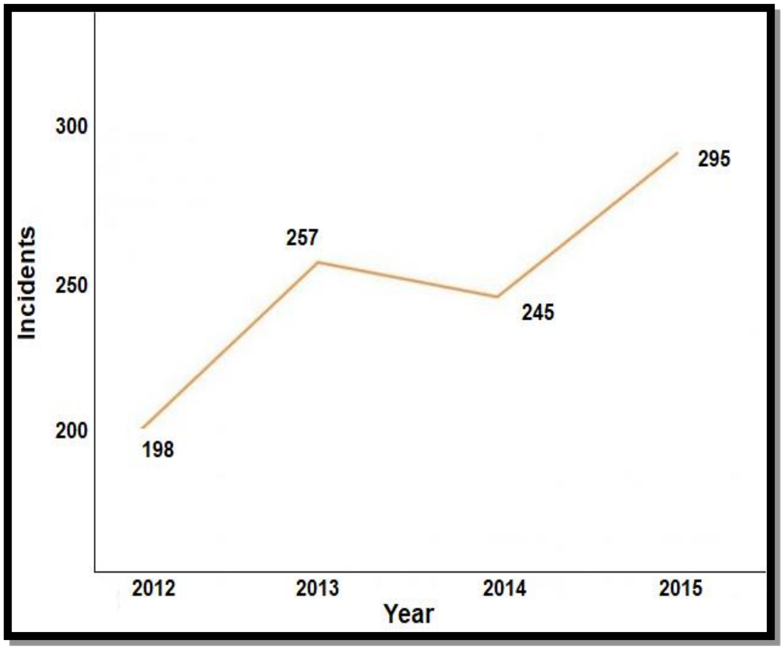


Figure 13. Reported number of cyber incidents against U.S. critical infrastructure from 2012 to 2015 (DHS).

The successful nuclear safety control system hack was only one of many attacks that serve as an example of the growing number of attacks the DHS reports on our critical infrastructure each year (Figure 13). If nation-states and other rogue organizations are interested in hacking our nation's infrastructure and our DoD networks, we must assume there is equal interest in gaining access to our world-class weapon systems. The key is to understand how long the nuclear safety control system remained offline for urgent, post-attack remediation and what required security modifications. Even in cases where a system is truly cyber-resilient and can function despite an attack, one must take near-immediate corrective action to patch the vulnerability to prevent a drain on resources or the hacker's ultimate success in infiltrating the system. Whether the system is resilient or requires shutting down to prevent damage or misuse, the program office must strive to minimize the time the system is down (Figure 14) or limited in functionality due to the vulnerability or compromised state (Arbaugh, Fithen, & McHugh, 2000).

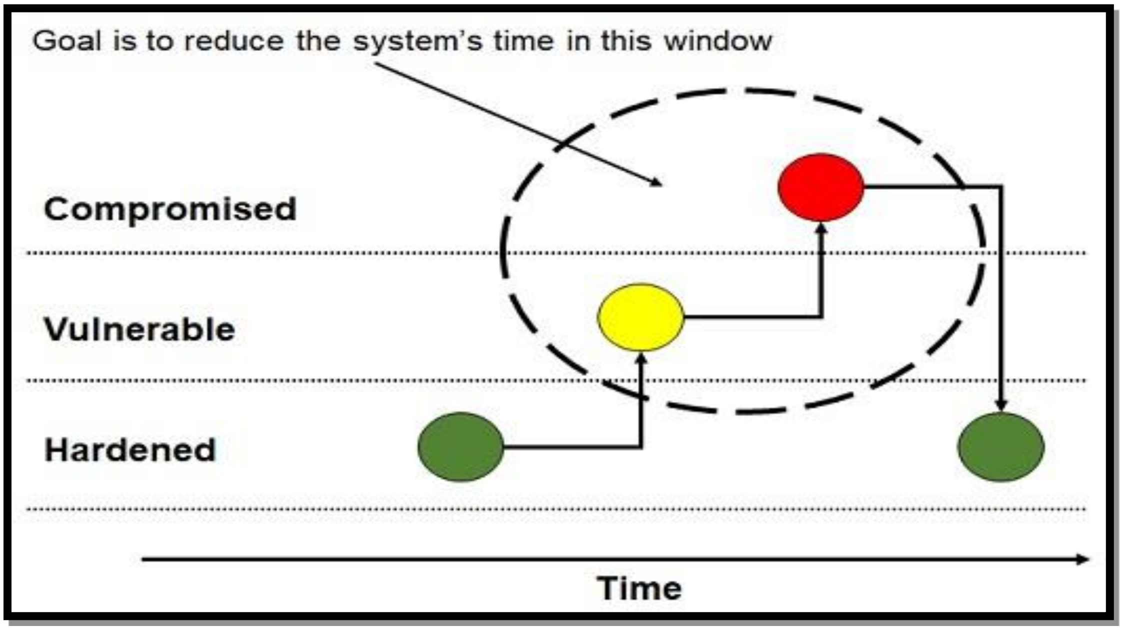


Figure 14. Minimizing vulnerable and compromised states (Arbaugh, Fithen, & McHugh, 2000).

A successful approach to developing cyber-resilient systems must include a variety of stakeholders—ranging from those who generate requirements to engineers, OEMs, program office and senior leadership—contributing to the effort. Hackers supported by terrorist organizations and nation-states employ a wide spectrum of approaches to gain access to our systems (Ranger, 2018). Many of these approaches are not limited to the direct users of the systems, as they are very likely to involve other stakeholders who provide support or development for these systems. Attacks using malware originating in email messages sent to individuals three and four layers removed from the system users are a common practice (Songer, 2018; DiMase et al., 2015).

Older systems have communication protocols that are not resistant to today's sophisticated cyber attacks. Various industries, including commercial airlines and the rail system, have recognized this fact. The railroad industry supports many legacy systems that are vulnerable to attacks that potentially impact their services and passenger safety (Upton, 2018). There are efforts underway, at significant costs, to provide detection and some methods for protective actions to keep the trains safe from these cyber threats. A significant number of our military systems used by our warfighters today use similarly outdated protocols and are not immune from the same methods hackers employ.

There exists a proliferation of knowledge on the hacker-side of the cyber equation, and their ingenuity is expanding to find ways and means to infiltrate virtually any device with computing capability, including medical devices, door locks, and solar panels (Palmer, 2018; Szoldra, 2016). There are hundreds of millions of devices in use today that can potentially become a point of attack for any other system, which further necessitates the need for cyber-resilient systems.

Research Methodology

Methodological Approach

Given the rapidly changing landscape of the cyber environment, the research of relevant documents and publications is primarily limited to those published between 2010 to the present. There are some instances of government documents published outside of these dates.

The research conducted is an extensive literature review of DoD and Army regulations, directives, instructions, and papers related to open systems and cybersecurity to gather a background on leader expectations in this area. The reviewed information covers current efforts in both military and industry to capture current methods for building and maintaining cyber-resilient systems. The use of available online sources provided for the discovery of cybersecurity-related information and best practices.

Additionally, the following sources for military resource information were utilized: Defense Technical Information Center (DTIC); Army Cyber Command (ARCYBER); Army Network Enterprise Technology Command (NETCOM); USCYBERCOM; Headquarters, Department of the Army (HQDA) CIO/G6; DoD CIO; and the Cyber Center of Excellence at Ft. Gordon. These sources provided the regulations, instructions, and policies as well as papers, briefings, research, and articles that cover cybersecurity, developing systems using open architectures, and standards.

For sources outside of the government, the following tools were employed: Google Scholar, Google Search, and the online libraries for three universities: Columbia College, Webster University, and University of Phoenix. The intended use of outside sources was to cover news about the DoD and services' use of open architecture as well as to determine best practices of industry in this area. These sources also afforded access to information on cyber threats and industry’s approaches to addressing their need for resiliency.

Data Collection

For this paper, the primary method for collecting data was a detailed search and analysis of relevant documents written on open systems, open architecture, cybersecurity, cyber threats, and cyber resiliency. The bulk of these documents were found online and in online databases. In addition to the online documents, some sources were in printed versions of journals and magazines. There are a limited number of references to conversations with leaders used to support the information shared in articles.

Validity of the Research

The documents selected come from a wide range of authors from academia, industry, and the DoD. This was purposefully done to provide a balanced look at the topic from a variety of vantage points and not taint the research from a single military or personal point of view.

Limitations of Study

Every effort was made to provide a detailed, well-balanced look at the problem; however, there are some limitations that prevented the collection of more data and a deeper analysis of the results. First, the paper’s due date prevented spending too much time conducting the amount of research necessary for a more in-depth look at an open system architecture’s impact on cyber resiliency. The reduced time, coupled with a full schedule of other requirements, such as seminars, book reviews, and travel for Senior Service College Fellowship (SSCF) classes, limited my ability to follow several references’ trails to build a more complete understanding of the authors’ rationale for the articles and papers used for this paper.

Another limitation was the restrictions on using surveys or interviews to gain the most current inputs of program managers, developers, users, and other key stakeholders for the weapon systems in use or under development. An attempt to overcome these restrictions was made by searching for the most recent articles and papers written by these individuals and using previous conversations or meetings in which their views were expressed.

Finally, to a certain extent, the timing of this study was a limitation. While open systems are not a new concept, it is not as readily adopted today as its availability might suggest. The same is true for the cybersecurity portion of the study. The DoD has modified the cybersecurity requirements several times to adjust to the rapidly changing cyber environment, but not much has been codified on the specific element of cyber resiliency. Many programs are working to meet the current RMF guidance in a post-production environment, which focuses on known—often outdated—threats. This means that the Army has been working predominantly with legacy systems built using proprietary architectures. There is little evidence available to provide a data-driven recommendation on the success levels that have been achieved by using open systems architectures.

Analysis and Findings

Summary of Findings

"We should seek to understand cyberspace in its own terms and avoid 'attempts to transfer policy constructs from other forms of warfare'" (Heftye, 2017, para. 11). Several authors reviewed in this research demonstrate this notion (Ranger, 2018; DiMase et al., 2015). In the past, the military forces have been able to see the capability threats our adversaries developed, which made the call to action for defense against them easier to initiate and support. Despite reading about successful cyber attacks against commercial organizations, such as Target, Home Depot, and Equifax, or against government organizations like the Office of Personnel Management (OPM) and the Internal Revenue Service (IRS), many DoD programs are not making the connections relating these threats to a hackers' ability to attack their weapon systems.

Setting aside the fact that these attacks were not directed against a military weapon system, one should note that attacks may have far-reaching impacts on the organizations that develop our weapons. Success in attacking those in the defense industry is well-documented. In one example, Lockheed Martin—a large weapon systems provider— discovered that its security tokens provided by RSA (initials of three founders, Ron Rivest, Adi Shamir, and Leonard Adleman) were compromised (Jackson, 2011). Had the company not discovered that attack, its network could have been compromised, ultimately bringing a lack of confidence in the security of the systems it provides.

The confidence in a system is paramount for users, as illustrated in a recent attack on Delta Airlines. The target of this attack was customer information, but the lasting impact was increased concern on impacts to the planes and the notion that this could halt operations (Songer, 2018). The Stuxnet attack on a controller in a nuclear plant that originated on the desktops of the part provider and the Delta Airlines attack clearly illustrate the understanding that a cyber threat against one type of system—in this case a customer support system—has the potential to migrate and attack other systems within the organization (Zetter, 2017; Songer 2018).

A system can survive when it achieves cyber resiliency and can continue to operate or quickly recover from a cyber-attack (DiMase et al., 2015). Meeting the ten CSAs found in the mandatory System Survivability KPP and successfully completing a series of testing events, beginning with table-top exercises against the proposed architecture and culminating in launching attacks against the system during operation testing, determines the ability of a system to weather a cyber attack. The system's ability to prevent, mitigate, and recover from these attacks at each stage needs to inform the design, development, and operation of the system at each stage of its lifecycle.

An analysis of the information uncovered in the literature review highlights the ability of a system developed using an open systems approach to more rapidly incorporate change or technology insertions. The research further reveals the high cost and extended time required to incorporate changes in a proprietary system with a single source provider. Given the rapid evolution of the cyber threats and the growing number of actors with desires to infiltrate our weapon systems, it is critical to have the capability to modify a system quickly and reduce the vulnerabilities that may prevent the warfighter from using the weapon.

There are many weapon system designs based on open architectures, which serve as positive examples to persuade any reluctant program managers who hear and act based upon emotional arguments and point to this approach having too many flaws and high costs that open systems are the right approach. The Army has demonstrated open systems architecture development works at the hardware and software levels of a weapon system. The CCDC

Aviation and Missile Center completed a successful test fire of the Modular Missile Technology (MMT-70), an aviation-designated lightweight missile developed with the MOSA construct to deliver a low cost and rapid modifications (AMRDEC Public Affairs, 2016). To further enable rapid enhancements, the software architecture allows for the addition of subsystem changes without modifying the source code of other subsystems for the missile (AMRDEC Public Affairs, 2016). The Navy is also showing successful implementations of open systems architectures in its Common Afloat Network & Enterprise Services (CANES), publishing a development stack for vendors to incorporate in providing open system capabilities on ships (Schmidt & Sledge, 2016).

In a proprietary system, the Army has no straightforward means of determining where the components originated or how crucial data is handled. Unfortunately, the Army typically discovers the origins after the system has been exploited and an investigation is conducted. The proprietary nature of the system thwarts our ability to rapidly adapt and counter cyber threats, making a vulnerability more exploitable and severely impacting mission effectiveness or readiness. Army leaders and engineers must break the paradigm that feeds this approach and move to partnerships focused on the use of open systems (Clinton, 2015).

Industry is leading the way in open systems architectures and partnering together to provide increased functionality and reduced costs. The automotive industry was an early advocate for open systems, beginning with the hardware components for vehicles. Customers repair their vehicles by using parts available from multiple manufacturers, because the automobile giants subscribe to a set of standards the parts suppliers also follow. In addition, the Boeing Dreamliner 787 uses an open architecture for its systems and works with numerous partners to provide these systems.

The partnering process succeeds when industry and government work together and develop the open systems approach based upon agreed standards (McCormick, Cohen, Hunter, & Sanders, 2018, Clinton 2015). In cases like the FACE^{TM} and SOSA^{TM} consortia, industry and the DoD benefit from the open systems approach, since more industry partners can compete to provide innovative solutions for the capabilities the services need. The services benefit by having more competitive pricing from their providers (Serbu, 2019).

This research opened awareness of the long-understood need for open systems as a means to reduce costs and development times. However, many articles illustrated that open systems approach adoption has been slow, despite several examples of success. There is a renewed focus on using open systems, and the requirement to make and keep our systems more survivable in a cyber-contested environment has boosted that need. Adoption of open systems is proven to reduce costs over time and enable more rapid development and integration of systems. For the purpose of cybersecurity, open systems provide the opportunity for more participants to have their innovative approaches for inserting cyber-resilient solutions into the architecture compete. The dark side of the cyber equation uses collaboration and sharing to enhance the tools and tactics to create malware or exploit vulnerabilities in systems, proving the power of many. This same thought process can be put into the development of cyber-resilient solutions.

Conclusion and Recommendations

Interpretation of Results

The Army must accept the fact that there will be cyber-attacks on its systems, and it is realistic to assume some will be successful. Reviewing the successful attacks in the commercial space tells us there is a growing appetite for hackers—including nation-states—to use cyber-based methods to steal information, deny use of systems, or engage in other destructive actions. Quantify the number of potential threats is extremely difficult, due to the rapidly growing and changing nature of the cyber environment (Dimase et al., 2015).

The information gathered in this research indicates the futility in spending resources on proprietary systems that employ a solution known only to the developer, as this increases the risk to the system. This study illustrates that a 100% guarantee that a system is secure is unobtainable, and Army program managers are better served by adopting a risk-based approach, leading them to be more cyber-resilient. In adopting an open systems approach and knowing there is a good chance of a successful cyber-attack, program managers can develop the system to minimize the negative impact and to allow for rapid remediation to secure the system and return to normal operations.

Meeting the System Survivability KPP requires a strong cybersecurity posture that is much more than passing a security scan and documenting the system’s vulnerabilities and mitigation strategies to obtain an ATO. This KPP goes beyond the initial fielding requirements, since the weapon system must be cyber-resilient while in the field. This is not something that can happen overnight; rather, cyber resiliency is achieved through a well-planned and designed architecture that is capable of being adapted to address newly discovered vulnerabilities and new, increasingly sophisticated cyber threats. Army weapons need well-trained users of the system to work the TTPs and fight through a cyber attack by recognizing the attack and performing actions to mitigate and recover the system to continue with the mission. A cyber-resilient system can limit the impact of an attack, mitigate the threat, improve the security posture, and return to normal operations.

Recommendations

The following recommendations, which are proposed for consideration, are a result of reviewing the literature from government and industry and conducting deliberate analysis of the advantages and disadvantages of open systems architecture.

Recommendation 1: The Defense Science Board, made up of about 50 retired senior military, government, and industry leaders, pointed out, “Areas to be pursued in the longer term should include: development of special purpose system architectures with inherent resilience, systematic analysis of potential modes of cyber vulnerability of systems, use of emerging technology developments for system resilience” (Gosler et al., 2013, p. 95). To achieve fielding systems with “inherent” resilience, which in turn helps the system to satisfy the System Survivability KPP, the Army must embrace and implement the adoption of open systems architecture at the foundation of the system design. Program and project managers must be more diligent in pursuing the open system approach codified in DoDD 5000.01 and DoDI 5000.02. Senior leaders across the DoD need to place more emphasis on open systems and cyber resiliency as part of the definition of a successful program and recognize the program and project managers who incorporate these architectures into their systems. Increased adoption of OSA will only occur at an increased pace if senior leadership champions the effort.

Recommendation 2: Every new start program, modification, or upgrade must include early design considerations for addressing requirements for the system’s ability to meet the

Cyber Survivability Attributes (CSA) to prevent attacks from cyber threats, mitigate attacks by detecting and responding to them, and quickly recover the system to full functionality. Each milestone decision of a new start or major upgrade should require documented evidence depicting the ten CSA attributes being addressed by the design or approved variance based upon a sound risk assessment weighed against the system's mission.   To accomplish this, the Army must train the acquisition workforce to understand the role it plays in the cybersecurity portion of system survivability, which we can accomplish by placing an emphasis on cybersecurity and the actions necessary for professionals taking classes in the Engineering, Test, Logistics, Contracting, and Finance career field courses within the current DAU curriculum. The entire team must be on board with cybersecurity if the system is going to meet the System Survivability KPP. The contracts must identify the CSAs as part of the requirements, and finance must budget for the work. The engineering teams for the services and industry must understand what they have to design and build to meet the CSAs intent. The test community must conduct rigorous testing at all levels to ensure it meets the System Survivability KPP. Users must understand how to operate the system and fight through cyber attacks using appropriate TTPs to keep their tactical advantage.

Recommendation 3: Engineering and technical courses conducted by DAU must incorporate more discussion and examples of success in using open systems architectures. Adding this discussion as part of the Systems Planning, Research, Development and Engineering (SPRDE); Information Technology (IT); and Program Management (PM) curricula at all levels will initiate an awareness of the value this approach brings over the lifecycle of the system. Education must be included as a foundational element of introducing change, given that much of the workforce learns from experience gained on the job. If incoming engineers, analysts, and scientists are gaining their practical knowledge primarily from an existing workforce that is operating based on experience and their personal comfort using proprietary solutions, they will propagate this philosophy to the next generation, and status quo will become the safe, comfortable choice.

Recommendation 4: Incoming program and project managers and deputy project managers are required to complete the DAU-provided Program Manager's Course - PMT 401. This is a valuable course, as it educates through a series of case studies from a variety of past program experiences. This course should be modified to include a segment on cybersecurity and spend time sharing examples of successful breaches in industry and the government. At the classified level, these discussions should include any specific instances of cyber-attacks on military weapon systems. The course would benefit by including special topic discussions on the Survivability KPP to include the specific importance of the ten Cyber Survivability Attributes that are essential in keeping a system operational in the event of a cyber attack. The course should include segments on open systems approaches to developing systems and must contain frank discussions on the advantages and disadvantages this approach provides to the various types of system development. Every program manager should enter his or her assignment with a solid understanding of the impacts a weak security architecture will have on his or her fielded systems.

Recommendation 5: Programs must take advantage of the numerous organizations, such as FACE^{TM} and SOSA^{TM}, to help understand the advantages of open system and learn how to incorporate them into contracting language. Program managers need to assign the appropriate technical and contracting professionals in their organizations and encourage their industry counterparts to join and attend meetings of organizations that work to develop standards for cybersecurity and open systems. Collaboration assists in formulating sound practices and further enhancements to make systems more secure and adaptable.

References

Air Force LCMC. (2018, September 24). FedRAMP Continuous monitoring strategy guide. Retrieved from https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

Alexander, K. (2013, August). The Army's way ahead in cyberspace. *Army Magazine*, *63*(8), 22-25.

AMRDEC Public Affairs. (2016, September 22). Modular open systems architecture missiles successfully test fired. Retrieved from www.army.mil/article/175563/modular_open_systems_architecture_missiles_successfully_test_fired

Anderson, T. (2018, December 12). They say software will eat the world. Here are some software bugs that took a stab at it. Retrieved from https://www.theregister.co.uk/2018/12/11/software_bugs_that_ate_the_world/

Arbaugh, W. A., Fithen, W. L., & McHugh, J. (2000). Windows of vulnerability: A case study analysis. *Computer.* Retrieved from http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf

Association of the U.S. Army News Staff. (2017, December 14). Policy, process limiting cyber effectiveness. *AUSA News*. Retrieved from www.ausa.org/news/policy-process-limiting-cyber-effectiveness

Basnight, Z., Butts, J., Lopez, J., & Dube, T. (2013). Analysis of programmable logic controller firmware for threat assessment and forensic investigation. Paper presented at the 9-VII.

Blau, J. (2004, May). Russia - a happy haven for hackers. *ComputerWeekly.com.* Retrieved from https://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers

Boland, R. (2016, August 26). Undersecretary of Defense visits U.S. Navy's cyber thought leaders. *Navy.mil.* Retrieved from www.navy.mil/submit/display.asp?story_id=96360

Bradley, T. (2018, December 12). How secure is security by obscurity? *Lifewire.* Retrieved from https://www.lifewire.com/security-through-obscurity-2486707

Bradley, T. (2018, May 4). New threat report highlights concerning malware trends. *Forbes.* Retrieved from www.forbes.com/sites/tonybradley/2018/05/04/new-threat-report-highlights-concerning-malware-trends/

Brantly, A. F. (2017). The violence of hacking: State violence and cyberspace. *The Cyber Defense Review,2*(1), 73-91.

Buley, T. (2012, July 13). Google's Android operating system is surprisingly bug-free. *Forbes*. Retrieved from https://www.forbes.com/sites/taylorbuley/2010/11/03/googles-android-operating-system-is-surprisingly-bug-free/#6a83273d5d72

Chaplain, C. T., Chitikila, R., Booth, B., Greifner, L., Holliday, L.T., Pfeiffer, K., … Wilson, R. (2018, October). *Weapon systems cybersecurity: DOD just beginning to grapple with scale of vulnerabilities: Report to the Committee on Armed Services, U.S. Senate* (128th ed., Vol. 19).

Clinton, Larry. (2015). Best practices for operating government-industry partnerships in cybersecurity. *Journal of Strategic Security, 8*(4), 53-68. dx.doi.org/10.5038/1944-0472.8.4.1456

Cochran, S. (2001, April 1). The rising costs of software complexity. Retrieved from http://www.drdobbs.com/the-rising-costs-of-software-complexity/184404575

Collier, C. P. (2017, January 24). Speech entitled: Hardware Open Systems Technology (HOST). Embedded Tech Trends, Bourbon Orleans Hotel, New Orleans, LA. Retrieved from embeddedtechtrends.com/2017/PDF_Presentations/T11A - HOST.pdf

Cooke, D. W. (2013). The resilience of the electric power delivery system in response to terrorism and natural disasters: Summary of a workshop. Retrieved from https://www.nap.edu/read/18535/chapter/4

Dattathreya, M. S., Cummings, B. P., & Sharafi, F. (2018, August 20). Reusable and Refresh-able: Open systems architecture for fighting vehicles. *Army.mil*. Retrieved from www.army.mil/article/210117/reusable_and_refresh_able_open_systems_architecture_for_fighting_vehicles

Daubenspeck, T. (2016, April). Building obsolescence–resistant systems: How to nip obsolescence in the bud. *DSP Journal*, *April/June*, 16-20. www.dsp.dla.mil/Portals/26/Documents/Publications/Journal/160401-DSPJ-03.pdf

Davis, S. (2018, January 26). Benefits of open platforms vs. proprietary platforms. [Web log post.] TED Systems, LLC. Retrieved from www.tedsystems.com/benefits-open-platforms-vs-proprietary-platforms/

Defense Acquisition University (n.d). LOG200 Intermediate Acquisition Logistics Lesson 2.5. Retrieved from http://cbafaculty.org/DAU/Intermediate%20Acquisition%20Logistics/LOG200_common_L2.5_pf_508.pdf

Department of Defense. (2003, May 15). *The Defense Acquisition System*. (DoD Directive 5000.01).

Department of Defense. (2015 January 7). *Operation of the Defense Acquisition System*. (DoD Instruction 5000.02).

Department of Defense (2018, September 18). *Summary of Department of Defense Cyber Strategy 2018*.

Department of Defense. (2018, April 25). *Cybersecurity Test and Evaluation Guidebook 2.0*.

Department of Defense. (2015, December 18). *Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)*. Retrieved from acqnotes.com/acqnote/acquisitions/jcids-manual-operations

Department of Defense, Chief Information Officer (DoD CIO). (2014, March 14). *Cybersecurity* (DoD Directive 8500.01).

Department of Defense, Chief Information Officer. (2014, March 12). *Risk Management Framework (RMF) for DoD Information Technology (IT)* (DoD Instruction 8510.01).

Department of Defense, Under Secretary of Defense (2015, April 19). *Implementation directive for Better Buying Power 3.0 – Achieving dominant capabilities through technical excellence and innovation.*

Department of Defense, Open Systems Architecture Data Rights Team. (2013). *DoD Open Systems Architecture: Contract guidebook for program managers* (v.1.1). Arlington, VA: Department of Defense.

Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics. (2015, May 26). *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle (v1.0).*

Department of the Army, CIO/G6. (2017). *Leaders Information Assurance / Cybersecurity Handbook*. Retrieved from www.army.mil/e2/c/downloads/299601.pdf

Department of the Army. (2013, June 25). Army Regulation AR25-1. Army Information Technology.

Department of the Army. (2007, October 24). Army Regulation AR25-2. Information Assurance.

Department of the Army. (2012). *Weapon systems 2012*. Washington, D.C.: ASA(ALT) Strategic Communications & Business Transformation.

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions, 35*(2), 291-300.

Dolan, C. (2016, November 7). Cybersecurity is a global threat to democracy, yet not well understood. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2016/11/07/cybersecurity-is-a-global-threat-to-democracy-yet-not-well-understood/#451596c45c2f

Finkle, J. (2017, December 14). Hackers halt plant operations in watershed cyber-attack. *Reuters.* Retrieved from www.reuters.com/article/us-cyber-infrastructure-attack/hackers-halt-plant-operations-in-watershed-cyber-attack-idUSKBN1E8271

Fisher, S. (2014, September 1). The proprietary trap. *Security today.* Retrieved from https://securitytoday.com/Articles/2014/09/01/The-Proprietary-Trap.aspx?Page=1

Fisher, T. (2019, April 12). Patch Tuesday: What it is & why you should care. Retrieved from https://www.lifewire.com/patch-tuesday-2625783

Foale, E. (2018). *Resilience reboot: Rethinking the cyber strategy* (Order No. 10748790). Available from ProQuest Dissertations & Theses Global. (2027473280). Retrieved from search-proquest-com.contentproxy.phoenix.edu/docview/2027473280?accountid=134061

Fritze, M., & Schiller-Wurster, K. (2018, January 16). Time to get serious about hardware cybersecurity. *Defense One.* Retrieved from www.defenseone.com/ideas/2018/01/time-get-serious-about-hardware-cybersecurity/145210/

Garbarino, Z. (2017, October 30). Task Force 1-28 receives OSRVT training. *Army.mil.* Retrieved from https://www.army.mil/article/196114/task_force_1_28_receives_osrvt_training

Government Accountability Office (GAO) (2013, July). *Defense acquisitions: DOD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly: Report to the Subcommittee on Tactical Air and Land Forces, Committee on Armed Services, House of Representatives* (GAO-13-651).

Government Accountability Office. (2017, February 15). *High-risk series: Progress on many high-risk areas, while substantial efforts needed on others: Report to congressional committees* (GAO-17-317). p. 248-268.

Gorman, S., Cole, A., & Dreazen, Y. (2009, April 21). Computer spies breach fighter-jet project. *The Wall Street Journal.* Retrieved from www.wsj.com/articles/SB124027491029837401

Gosler, J. R., & Von Thaer, L. (2013). *Resilient military systems and the advanced cyber threat*. Washington, DC: Defense Science Board.

Greenberg, A. (2017, June 13). 'Crash Override': The malware that took down a power grid. *WIRED.* Retrieved from www.wired.com/story/crash-override-malware/

Gregg, A. (2018, October 14). Defense industry grapples with cybersecurity flaws in new weapons systems. *The Washington Post.* Retrieved from https://www.washingtonpost.com/business/economy/defense-industry-grapples-with-cybersecurity-flaws-in-new-weapons-systems/2018/10/14/b1de3bae-ce36-11e8-a360-85875bac0b1f_story.html?utm_term=.74fa710e7dad

Guertin, N. (2018, October 15). Emerging opportunities in modularity and open systems architectures. Retrieved from https://insights.sei.cmu.edu/sei_blog/2018/10/emerging-opportunities-in-modularity-and-open-systems-architectures.html

Hawkins, D. (2018, October 10). The Cybersecurity 202: The Pentagon's new weapons systems are vulnerable to cyberattacks, government watchdog finds. Retrieved from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/10/10/the-cybersecurity-202-the-pentagon-s-new-weapons-systems-are-vulnerable-to-cyberattacks-government-watchdog-finds/5bbcdf681b326b7c8a8d18dd/?utm_term=.b7179b10c739

Hayes, D. (2017, October 10). Security through obscurity is not security at all • WPShout. Retrieved from https://wpshout.com/security-through-obscurity/

Haynes, L. (2013, October 16). 5D robotics answers military's mandate for interoperability in future robots. *U.S. Newswire*. Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1442202663?accountid=35812

Heftye, E. (2017). Multi-Domain confusion: All aomains are not created equal. *The Strategy Bridge*. thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal

Held, G. (2006). Proprietary (closed) architecture. In *Dictionary of communications technology: terms, definitions and abbreviations.* Hoboken, NJ: Wiley. Retrieved from https://search-credoreference-com.contentproxy.phoenix.edu/content/entry/hmhighdef/closed_architecture/0

Heusel, D. D. (2017, August 15). Hill, Robins to provide F-35 software sustainment. *Hill Air Force Base.* Retrieved from https://www.hill.af.mil/News/Article-Display/Article/1279064/hill-robins-to-provide-f-35-software-sustainment/

Honkus, F. (2015). Presentation entitled: A need for Tactics, Techniques, and Procedures (TTP). USCYBERCOM. Retrieved from https://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_169626.pdf

Huda, S., Alyahya, S., Ali, M. M., Ahmad, S., Abawajy, J., Al-Dossari, H., & Yearwood, J. (2018). A Framework for software defect prediction and metric selection. *IEEE Access,6*, 2844-2858. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8240899

Irwin, L. (2018, March 23). 6 reasons why software is becoming more vulnerable to cyber-attacks. [Web log post]. it governance. Retrieved from www.itgovernance.eu/blog/en/6-reasons-why-software-is-becoming-more-vulnerable-to-cyber-attacks

Jackson, W. (2011, June 7). RSA confirms its tokens used in Lockheed hack. Retrieved from https://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx

Jackson, W. (2018, April 02). New risk management framework expected to improve DoD cybersecurity. *Federal News Network.* Retrieved from https://federalnewsnetwork.com/cyber-exposure/2018/04/using-the-risk-management-framework-to-improve-cybersecurity/

Jordan, L. H., Jr., & Boudreau, V. (2013). *Cyber Infrastructure Protection.* (Vol. 2, Rep.). (T. Saadawi, Ed.). Carlisle, PA: U.S. Army War College Press.

Keeney, K. (2018, August 16). *Why open-sourced code can boost cybersecurity*. *Fifth Domain.* Retrieved from www.fifthdomain.com/thought-leadership/2018/08/16/why-open-sourced-code-can-boost-cybersecurity/

Kendall, F. (2017, December 15). Terms of Reference - Survivable Logistics. [Letter written to Chairman, Defense Science Board]. Retrieved from www.acq.osd.mil/dsb/tors/TOR-2016-12-15-Survivable_Logistics.pdf

Krebs, B. (2017, June 17). Why so many top hackers hail from Russia. *Krebs on Security*. Retrieved from https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/

Kumar, M. (2015, March 20). China finally admits it has army of hackers. *The Hacker News.* Retrieved from https://thehackernews.com/2015/03/china-cyber-army.html

Lacdan, J. (2018, November 02). Interoperability a key focus in building the Army's future network. Retrieved from https://www.tradoc.army.mil/Publications-and-Resources/Article-Display/Article/1675457/interoperability-a-key-focus-in-building-the-armys-future-network/

Lamolinara, V. (2018, June 6). Lecture entitled: Cybersecurity as it applies to the survivability Key Performance Parameter. DAU - Mid-Atlantic Region, Aberdeen. Retrieved from https://www.dau.mil/Lists/Events/Attachments/104/06-06-2018_Cyber Survivability Webinar Final with resources UTM.pdf

Lange, K. (2018, October 2). DOD's Cyber Strategy: 5 Things to Know. *U.S. Dept. of Defense.* Retrieved from www.defense.gov/explore/story/Article/1648425/dods-cyber-strategy-5-things-to-know/

Lindros, K. (2016, October 12). 12 hardware and software vulnerabilities you should address now. *CIO.* Retrieved from www.cio.com/article/3129347/security/12-hardware-and-software-vulnerabilities-you-should-address-now.html

Loeb, L. (2018, February 19). Microsoft vulnerabilities more than doubled in 2017 - Report. *Security Now.* Retrieved from https://www.securitynow.com/author.asp?section_id=649&doc_id=740671

Malekzadeh, R. (2014). The advent of decoupling of hardware and software. *CIO Review.* Retrieved from https://networking.cioreview.com/cxoinsight/the-advent-of-decoupling-of-hardware-and-software-nid-11-cid-9.html

Manning, B. (2017, July 17). Open-Standard System Architecture. *AcqNotes.* Retrieved from http://acqnotes.com/acqnote/careerfields/open-standard-system-architecture

Mansfield, K., Eveleigh, T., Holzer, T. H., & Sarkani, S. (2015). DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model. *Defense AR Journal, 22*(2), 240-273.

Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. Lincoln: Potomac Books.

McCormick, R., Cohen, S., Hunter, A. P., & Sanders, G. (2018, March). National Technology and Industrial Base Integration. Retrieved from https://www.csis.org/analysis/national-technology-and-industrial-base-integration

Meola, A. (2016, May 26). Cyber attacks against our critical infrastructure are likely to increase. *Business Insider*. Retrieved from www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5

Merriam-Webster. (n.d.). Cyber attack. On Merriam-webster.com. Retrieved from https://www.merriam-webster.com/dictionary/cyberattack

Midrack, L. (2018, December 12). What is Open Source Software? Retrieved from https://www.lifewire.com/what-is-open-source-software-4147547

MITRE. (2015, April 10). System Architecture. *MITRE.* Retrieved from www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/system-architecture

Moore, M. S. (2016, April). Modular Open System Architectures (MOSA) for Military Systems. Retrieved from https://www.researchgate.net/profile/Michael_Moore14/publication/302936381_Modular_Open_System_Architectures_MOSA_for_Military_Systems_Addressing_Challenges_of_Complex_Systems/links/5733af0b08ae298602dcefdd.pdf?origin=publication_detail

Murray, Hurcules. (n.d.). Cyber Requirements. Retrieved from https://www.afcea.org/events/augusta/14/documents/T2S2AFCEATechnetCyberRequirements.pdf

Murray, Randy. (2012, March 19). Intellectual Property and Technical Data Rights: “It’s About the Money.”, U.S. Army War College Research Paper. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a593245.pdf

Norton, J. (2015). Enhancing Interoperability through Open Systems Architecture. *Defense Standardization Program Journal,* (October-December), 11-16.

Oberndorf, T., & Sledge, C. (2010). Open Systems: What’s Old Is New Again. Retrieved from https://resources.sei.cmu.edu/asset_files/Presentation/2010_017_001_22271.pdf

Office of the Deputy Assistant Secretary of Defense (ODASD) - Systems Engineering. (2017, October 7). Modular Open Systems Approach. *ODASD.* Retrieved from www.acq.osd.mil/se/initiatives/init_mosa.html

Open Group, FACE Consortium (Comp.). (2017, March). *Future Airborne Capability Environment (FACE™) Technical Standard, Edition 3.0* [Technical Standards]. Burlington, MA.

Palmer, D. (2018, March 15). IoT security warning: Cyber-attacks on medical devices could put patients at risk. *ZDNet.* Retrieved from www.zdnet.com/article/iot-security-warning-cyber-attacks-on-medical-devices-could-put-patients-at-risk/

Park, D., Summers, J., & Walstrom, M. (2017, October 11). Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. Retrieved from https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Pellerin, C. (2014, November 5). Open Architecture Cuts Cost, Promotes Competition, Official Says. Retrieved from https://dod.defense.gov/News/Article/Article/603587/

Perlroth, N. and Sanger, D. E. (2013, July 13). Nations Buying as Hackers Sell Flaws in Computer Code. *The New York Times.* Retrieved from www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

Ranger, S. (2018, December 04). What is cyberwar? Everything you need to know about the frightening future of digital conflict. *ZDNet.* Retrieved from https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Rani, C., Modares, H., Sriram, R., Mikulski, D., & Lewis, F. L. (2016). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation*, *13*(3), 331–342.

Rempfer, K. (2018, July 05). Abrams tanks get new round of Israeli-made 'shields' to fend off anti-tank weapons. *Army Times.* Retrieved from www.armytimes.com/news/2018/07/05/abrams-tanks-get-new-round-of-israeli-made-shields-to-fend-off-anti-tank-weapons/

Rutkowski, R. (2019, March 12). What is a DoD Modular Open Systems Approach (MOSA)? (5 Core Principles). Retrieved from https://blog.bliley.com/what-is-a-dod-modular-open-systems-approach-mosa

Schmidt, D. C. (2014, November 15). Why Software Reuse Has Failed and How to Make It Work for You. *Vanderbilt.* Retrieved from www.dre.vanderbilt.edu/~schmidt/reuse-lessons.html

Schmidt, D. C. (2013, October 10). Lecture entitled: Applying Agility to DoD Software Initiatives. IEEE Computer Society Lockheed Martin Webinar Series. Retrieved from www.computer.org/cms/Computer.org/webinars/lmco/10102013Slides-Schmidt.pdf

Schmidt, D. C., & Sledge, C. (2016, July 11). A Naval Perspective on Open-Systems Architecture. *Carnegie Mellon University*. Retrieved from https://insights.sei.cmu.edu/sei_blog/2016/07/a-naval-perspective-on-open-systems-architecture.html

Seals, T. (2018, January 26). Cyber attacks Doubled in 2017. *info security*. Retrieved from www.infosecurity-magazine.com/news/cyber attacks-doubled-in-2017/

Secureworks. (2017, May 12). Cyber Threat Basics, Types of Threats, Intelligence & Best Practices. Retrieved from https://www.secureworks.com/blog/cyber-threat-basics

SEI Pocast Series. (2015, October 19). Open Systems Architectures: When & Where to Be Closed. [Podcast transcription]. Carnegie Mellon University Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/Podcast/2016_016_100_453909.pdf

Serbu, J. (2019, February 11). In military services, new push from the top toward open systems architectures. *Federal News Network.* Retrieved from https://federalnewsnetwork.com/defense-main/2019/02/in-military-services-new-push-from-the-toward-open-systems-architectures/

Serbu, J. (2013, November 13). DoD brings culture of open architecture to a world of proprietary systems. *Federal News Network.* Retrieved from federalnewsnetwork.com/defense/2013/11/dod-brings-culture-of-open-architecture-to-a-world-of-proprietary-systems/

Shaffer, R.M. (2015, February). Why Software Firms Build Hardware – And What Microsoft Is Doing About It. *Massachusetts Institute of Technology*. Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/100312/932078071-MIT.pdf;sequence=1

Sheets, D. (2018, September 26). Decomposing system security to prevent cyber attacks in trusted computing architectures. *Military & Aerospace Electronics.* Retrieved from https://www.militaryaerospace.com/articles/2018/09/trusted-computing-system-security-cyber-attacks.html

Sholtis, J. (2017, June 16). Empowering DOD with critical cyber training. *FCW.* Retrieved from https://fcw.com/articles/2017/06/16/comment-sholtis-cyber-training.aspx

Significant Cyber Incidents. (2018, October). *Center for Strategic & International Studies.* Retrieved from www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Simi, S. (n.d.). Growth of Software Complexity in Commercial Aircraft. *System Architecture Virtual Integration.* Retrieved from https://savi.avsi.aero/about-savi/savi-motivation/exponential-system-complexity/

Sledge, C. (2015, November 23). A Discussion on Open-Systems Architecture. *Carnegie Mellon University*. Retrieved from https://insights.sei.cmu.edu/sei_blog/2015/11/a-discussion-on-open-systems-architecture.html

Sobers, R. (2019, April 17). 60 Must-Know Cybersecurity Statistics for 2019. Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/

Songer, D. (2018, April 12). Airline security a cause for concern, as Delta reveals 2017 cyber attack. *Transport Security World.* Retrieved from www.transportsecurityworld.com/airline-security-delta-reveals-2017-cyber attack

South, T. (2017, October 25). Army receives upgraded Abrams tank — and more improvements are on the way. *Army Times.* Retrieved November 13, 2018, from www.armytimes.com/news/your-army/2017/10/25/army-receives-upgraded-abrams-tank-and-more-improvements-are-on-the-way/

Sprenger, S. (2018, November 14). US Air Force moves to fortify F-35 weak points against hacking. *Air Force Times.* Retrieved from www.airforcetimes.com/air/2018/11/14/us-air-force-moves-to-fortify-f-35-weak-points-against-hacking/

Statista. (2018). Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions). *Statista.* Retrieved from www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Stecklein, J. M. (2004). Error Cost Escalation Through the Project Life Cycle - NASA. Retrieved from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100036670.pdf

Such, G., Gagliardi, M., & Woody, C. (2015, November 12). Presentation on the theme: NDIA INCOTE Introduction to the SEI. Carnegie Mellon University, Pittsburgh, PA. Retrieved from https://slideplayer.com/slide/12045898/

Suits, D. L. (2018, November 30). Cyber-strategy competitions helping develop future leaders. *Army.mil.* Retrieved from www.army.mil/article/214508/cyber_strategy_competitions_helping_develop_future_leaders

Szoldra, P. (2016, October 21). Here's how the 'Internet of Things' is being used for major cyber attacks on corporations. *Buisiness Insider.* Retrieved from www.businessinsider.com/internet-of-things-corporate-cyber attacks-2016-10

Thomson, I. (2018, April 17). So, you've got a zero-day – do you sell to black, grey or white markets? *The Register.* Retrieved from https://www.theregister.co.uk/2018/04/15/mature_bug_bounty_market_bsidessf/

Tokar, J. (2017, March). An Examination of Open System Architectures for Avionics Systems. *Research Gate.* Retrieved from www.researchgate.net/profile/Joyce_Tokar/publication/315736224_An_Examination_of_Open_System_Architectures_for_Avionics_Systems_-_An_Update/links/58e022fb92851c3695490509/An-Examination-of-Open-System-Architectures-for-Avionics-Systems-An-Update.pdf?origin=publication_detail

The United States of America, President of the United States. (2018). *National Cyber Strategy of the United States of America*. Washington, DC: White House.

Upton, L. (2018, January 25). "Train attacks are no longer science fiction," declares startup after raising $4.7M to protect rail and metro from cyber attacks. *Transport Security World.* Retrieved from www.transportsecurityworld.com/train-attacks-are-no-longer-science-fiction-declares-startup-after-raising-4.7m-to-protect-rail-and-metro-from-cyber-attacks

Vijay. (2018, June 07). Alpha Testing and Beta Testing: A Complete Guide. *Software Testing Help.* Retrieved from https://www.softwaretestinghelp.com/what-is-alpha-testing-beta-testing/

Warshawsky, D. S. (2015). A System-of-Systems Flexibility Framework: A Method for Evaluating Designs that are Subjected to Disruptions. *Georgia Institute of Technology*. Retrieved November 21, 2018, from smartech.gatech.edu/bitstream/handle/1853/54277/Warshawsky-Dissertation-2015.pdf

Wigginton, S., & Jacobs, W. (2018, August). Strength in Architecture. *Army AL&T Magazine*, (Special), 53-57.

Wilson, C. (2000, September 22). 15-Year-Old Admits Hacking NASA Computers. *abc News.* Retrieved from https://abcnews.go.com/Technology/story?id=119423&page=1

Wong, W. (2013, June 11). Interview: The Open Group's Judy Cerenzia Discusses The Future Airborne Capability Environment. *Electronic Design.* Retrieved from https://www.electronicdesign.com/embedded/interview-open-group-s-judy-cerenzia-discusses-future-airborne-capability-environment

Xie, M. (2018, March 13). Moore's Law at Warp Speed: The Global Security Risks of a Post-Quantum World. *Forbes.* Retrieved from www.forbes.com/sites/forbestechcouncil/2018/03/13/moores-law-at-warp-speed-the-global-security-risks-of-a-post-quantum-world/

Zetter, K. (2017, June 03). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *WIRED.* Retrieved from www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zimmerman, P. (2018, July 12). Modular Open Systems Approach (MOSA) Panel on Standards Retrieved from https://www.dsp.dla.mil/Portals/26/Documents/Publications/Conferences/2018/DSP%20

Workshop%20July2018/DSPWorkshop-Day4-180712/DSPWorkshop-1Zimmerman-180712.pdf?ver=2018-08-01-150711-883

Zimmerman, P. (2015, October 27). Modularity and Open Systems: Meaningful Distinctions. Retrieved from https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2015/system/17983_Zimmerman.pdf

Appendix A: Acronyms

ADD	Aviation Development Directorate
AMD	Advanced Micro Devices
AMRDEC	Aviation and Missile Research, Development and Engineering Command
ARCYBER	Army Cyber Command
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics & Technology)
ATO	Authority to Operate
AvMC	Aviation and Missile Center (formerly AMRDEC)
BBP	Better Buying Power
C4I	Command, Control, Communications, Computers, and Intelligence
CANES	Common Afloat Network & Enterprise Services
CBRN	Chemical, Biological, Radiological and Nuclear
CCDC	Combat Capabilities Development Command (formerly RDECOM)
CDD	Capability Development Documents
CIO	Chief Information Officer
COTS	Commercial off the Shelf
CPU	Central Processing Unit
CSA	Cyber Survivability Attributes
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DAU	Defense Acquisition University
DCGS	Distributed Common Ground System
DHS	Department of Homeland Security
DSB	Defense Science Board
DTIC	Defense Technical Information Center
FACE™	Future Airborne Capability Environment
GAO	Government Accountability Office
GPS	Global Positioning System

GCS	Ground Control Station
HOST	Hardware Open Systems Technology
HQDA	Headquarters Department of the Army
HVAC	Heating, Ventilation, and Air Conditioning
IMA	Integrated Modular Avionics
IP	Internet Protocol
IRS	Internal Revenue Service
IT	Information Technology
JBC-P	Joint Battle Command - Platform
JCIDS	Joint Capabilities Integration and Development System
JCS	Joint Chiefs of Staff
JSF	Joint Strike Fighter
JTRS	Joint Tactical Radio System
KPP	Key Performance Parameter
MG(R)	Major General (Retired)
MMT	Modular Missile Technology
MOSA	Modular Open System Architecture
NASA	National Aeronautics and Space Administration
NAVAIR	Naval Air Systems Command
NETCOM	Army Network Enterprise Technology Command
NIPR	Non-classified Internet Protocol Router
OA	Open Architecture
ODASD	Office of the Deputy Assistant Secretary of Defense
OEM	Original Equipment Manufacturer
OPM	Office of Personnel Management
ORD	Operation Requirements Documents
OSA	Open System Architecture
OSRVT	One System Remote Video Terminal
PEO	Program Executive Office
PLC	Programmable Logic Controllers

PM	Program (or Project) Manager
RMF	Risk Management Framework
SBIR	Small Business Innovation Research
SLOC	Source Lines of Code
SoS	System of Systems
SOSA^{TM}	Sensor Open Systems Architecture
SPAWAR	Space and Naval Warfare Systems Command
SPRDE	Systems Planning, Research, Development and Engineering
SSCF	Senior Service College Fellowship
SSL	Secure Socket Layer
STEM	Science, Technology, Engineering, and Math
TTP	Tactics, Techniques, and Procedures
UAS	Unmanned Aerial System
UDP	User Datagram Protocol
USB	Universal Serial Bus
USCYBERCOM	United States Cyber Command
USD(AL&T)	Under Secretary of Defense (Acquisition, Logistics & Technology)